Manual do Usuário

KASPERSKY INTERNET SECURITY 2009

Caro usuário do Kaspersky Internet Security 2009,

Obrigado por escolher nosso produto. Esperamos que esta documentação o ajude em seu trabalho e forneça as respostas referentes ao software.

Este documento pode ser alterado sem aviso prévio. Para obter a versão mais recente, consulte o site da Kaspersky Lab em http://www.kaspersky.com.br/docs. A Kaspersky Lab não assume qualquer responsabilidade pelo conteúdo, qualidade, relevância ou precisão do material usado neste documento cujos direitos são de propriedade de terceiros ou por danos potenciais associados ao uso de tais documentos.

+7 (495) 645-7939,
Fone, Fax: +7 (495) 797-8700,
+7 (495) 956-7000

http://www.kaspersky.com.br/
http://support.kaspersky.com/

Data de revisão: 13.11.2008

SUMÁRIO

INTRODUÇÃO 6
Obtendo informações sobre o aplicativo 6
Fontes de informações para pesquisar sozinho 6
Para entrar em contato com o Departamento de Vendas 7
Para entrar em contato com o Serviço de Suporte Técnico 7
Discutindo os aplicativos da Kaspersky Lab no fórum da Web 9
Novidades do Kaspersky Internet Security 2009 9
Visão geral da proteção do aplicativo 11
Assistentes e ferramentas 12
Recursos de suporte 13
Análise heurística 14
Requisitos de hardware e software do sistema 15
AMEAÇAS À SEGURANÇA DO COMPUTADOR 17
Aplicativos de ameaça 17
Programas maliciosos 18
Vírus e worms 18
Cavalos de Tróia 22
Utilitários maliciosos 28
Programas potencialmente indesejados 32
Adware 33
Pornware 33
Outros programas de Riskware 34
Métodos de detecção de objetos infectados, suspeitos e potencialmente perigosos pelo aplicativo 38
Ameaças da Internet 39
Spam ou e-mails recebidos não-solicitados 39
Phishing 40
Ataques de hackers 40
Banners 41
INSTALANDO O APLICATIVO 42
Etapa 1. Pesquisando uma versão mais recente do aplicativo 43

Etapa 2. Verificando se o sistema atende aos requisitos de instalação....... 44
Etapa 3. Janela de boas-vindas do assistente 44
Etapa 4. Exibindo o Contrato de Licença 45
Etapa 5. Selecionando o tipo de instalação 45
Etapa 6. Selecionando a pasta de instalação 46
Etapa 7. Selecionando os componentes do aplicativo a serem instalados .. 46
Etapa 8. Procurando outros aplicativos antivírus...................................... 47
Etapa 9. Preparação final para a instalação... 48
Etapa 10. Concluindo a instalação 49

INTERFACE DO APLICATIVO 50
Ícone da área de notificação 50
Menu de atalho 51
Janela principal do aplicativo 53
Notificações 56
Janela de configurações do aplicativo 56

INTRODUÇÃO 58
Selecionando o tipo de rede 59
Atualizando o aplicativo 60
Análise de segurança 60
Verificando vírus no computador... 61
Gerenciando a licença 62
Assinatura para renovação automática da licença 63
Participando do Kaspersky Security Network.. 65
Gerenciamento de segurança 67
Pausando a proteção.. 69

VALIDANDO AS CONFIGURAÇÕES DO APLICATIVO 71
Testar o "vírus" da EICAR e suas modificações.. 71
Testando a proteção do tráfego HTTP 75
Testando a proteção do tráfego SMTP.. 76
Validando as configurações de Arquivos e memória 76
Validando as configurações da tarefa de varredura de vírus 77
Validando as configurações do Anti-Spam 78

DECLARAÇÃO SOBRE COLETA DE DADOS DO KASPERSKY SECURITY NETWORK 79

KASPERSKY LAB 85

CRYPTOEX LLC 88

MOZILLA FOUNDATION 89

CONTRATO DE LICENÇA 90

INTRODUÇÃO

NESTA SEÇÃO:

Obtendo informações sobre o aplicativo 6

Novidades do Kaspersky Internet Security 2009 9

Visão geral da proteção do aplicativo 11

Requisitos de hardware e software do sistema 15

OBTENDO INFORMAÇÕES SOBRE O APLICATIVO

Se houver dúvidas sobre a compra, a instalação ou o uso do aplicativo, você pode obter respostas imediatamente.

A Kaspersky Lab possui diversas fontes de informação e você pode selecionar a mais conveniente, dependendo da urgência e da importância de sua pergunta.

FONTES DE INFORMAÇÕES PARA PESQUISAR SOZINHO

Você pode utilizar o sistema de **Ajuda**.

O sistema de Ajuda contém informações sobre o gerenciamento da proteção do computador: como exibir o status de proteção, verificar diversas áreas do computador e executar outras tarefas.

Para abrir a Ajuda, clique no link **Ajuda** na janela principal do aplicativo ou pressione **<F1>**.

Para entrar em contato com o Departamento de Vendas

Se houver dúvidas sobre a seleção ou a compra do aplicativo ou sobre como prorrogar seu período de utilização, telefone para os especialistas do Departamento de Vendas em nosso escritório central em Moscou nos números:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**.

O serviço é fornecido em russo ou em inglês.

Você pode enviar suas dúvidas para o Departamento de Vendas através do e-mail sales@kaspersky.com.

Para entrar em contato com o Serviço de Suporte Técnico

Se você já tiver comprado o aplicativo, poderá obter informações sobre o mesmo junto ao Serviço de Suporte Técnico por telefone ou através da Internet.

Os especialistas do Serviço de Suporte Técnico responderão suas perguntas sobre a instalação e o uso do aplicativo e, caso o seu computador tenha sido infectado, eles o ajudarão a eliminar as conseqüências das atividades de malware.

Antes de entrar em contato com o Serviço de Suporte Técnico, leia as regras de suporte (http://support.kaspersky.com/support/rules).

Solicitação de Serviço de Suporte Técnico por e-mail (apenas para usuários registrados)

> Você pode fazer a sua pergunta aos especialistas do Serviço de Suporte Técnico preenchendo um formulário do Helpdesk na Web (http://support.kaspersky.com/helpdesk.html).
>
> Você pode enviar sua pergunta em russo, inglês, alemão, francês ou espanhol.

Para enviar um e-mail com a sua dúvida, indique o **número do cliente** obtido ao registrar-se no site do Serviço de Suporte Técnico, juntamente com a sua **senha**.

> Observação
>
> Se você ainda não for um usuário registrado dos aplicativos da Kaspersky Lab, poderá preencher um formulário de registro em https://support.kaspersky.com/en/PersonalCabinet/Registration/Form/. Durante o registro, você deverá fornecer o código de ativação ou o nome do arquivo de chave.

O Serviço de Suporte Técnico responderá à sua solicitação no seu **Gabinete Pessoal** em https://support.kaspersky.com/en/PersonalCabinet) e através do endereço de e-mail especificado na sua solicitação.

Descreva o problema encontrado no formulário de solicitação da Web com o máximo de detalhes possível. Especifique as seguintes informações nos campos obrigatórios:

- **Tipo de solicitação**. As perguntas mais freqüentes feitas pelos usuários estão agrupadas em tópicos específicos, por exemplo: “Problema de instalação/remoção de produto” ou “Problema de varredura/remoção de vírus”. Se não houver um tópico correspondente à sua dúvida, selecione “Pergunta geral”.

- **Nome do aplicativo e número da versão**.

- **Texto da solicitação**. Descreva o problema encontrado com o máximo de detalhes possível.

- **Número do cliente e senha**. Digite o número de cliente e a senha recebidos durante o registro no site do Serviço de Suporte Técnico.

- **Endereço de e-mail**. O Serviço de Suporte Técnico enviará a resposta para este endereço de e-mail.

Suporte Técnico por telefone

Se você tiver um problema e precisar de ajuda urgente, poderá telefonar para o escritório de Suporte Técnico mais próximo. Será necessário fornecer suas informações de identificação (http://support.kaspersky.com/support/details) ao solicitar Suporte Técnico em russo (http://support.kaspersky.com/support/support_local) ou internacional (http://support.kaspersky.com/support/international). Isto

ajudará nossos especialistas a processar sua solicitação com a maior rapidez possível.

DISCUTINDO OS APLICATIVOS DA KASPERSKY LAB NO FÓRUM DA WEB

Se a sua dúvida não precisar de uma resposta urgente, você poderá discuti-la com os especialistas da Kaspersky Lab e com outros usuários de software Kaspersky no nosso fórum, em http://forum.kaspersky.com/.

Neste fórum, você pode ver os tópicos existentes, deixar suas respostas, criar novos tópicos e usar o mecanismo de pesquisa.

NOVIDADES DO KASPERSKY INTERNET SECURITY 2009

O Kaspersky Internet Security 2009 (também chamado de "Kaspersky Internet Security" ou "o aplicativo") aborda a segurança de dados de uma forma totalmente nova, baseada na restrição dos direitos de acesso de cada programa aos recursos do sistema. Essa abordagem ajuda a evitar ações indesejadas por programas suspeitos e perigosos. A capacidade do aplicativo de proteger os dados confidenciais de cada usuário também foram consideravelmente aprimorados. Agora, o aplicativo inclui assistentes e ferramentas que simplificam significativamente as tarefas específicas de proteção do computador.

Segue uma análise dos novos recursos do Kaspersky Internet Security 2009:

Novos recursos de proteção:

- Agora, o Kaspersky Internet Security inclui os componentes Filtragem de Aplicativos, Defesa Proativa e Firewall que, juntos, implementam uma nova abordagem integrada à proteção do sistema contar ameaças conhecidas e desconhecidas. Agora, com a utilização de listas de aplicativos confiáveis ("listas brancas"), o Kaspersky Internet Security exige muito menos participação do usuário.
- A varredura do sistema operacional e do software instalado para detectar e eliminar vulnerabilidades mantém um alto nível de segurança do sistema e evita que programas perigosos invadam seu sistema.

- Os novos Assistentes do Analisador de Segurança e de Configuração do Navegador facilitam a verificação e a eliminação de ameaças e vulnerabilidades de segurança nos aplicativos instalados, e a configuração do sistema operacional e do navegador.

- Agora, a Kaspersky Lab reage mais rápido às novas ameaças com o uso do Kaspersky Security Network, que coleta dados sobre a infecção de computadores de usuários e os envia aos servidores da Kaspersky Lab.

- Novas ferramentas – Monitor de Rede e Análise de Pacotes de Rede - facilitam a coleta e a análise de informações sobre as atividades de rede no seu computador.

- O novo Assistente de Restauração do Sistema ajuda a reparar os danos ao sistema causados por ataques de malware.

Novos recursos de proteção de dados confidenciais:

- O novo componente Filtragem de Aplicativos monitora com eficiência o acesso a dados confidenciais, arquivos do usuário e pastas de aplicativos.

- A nova ferramenta Teclado Virtual assegura a segurança de dados confidenciais digitados no teclado.

- O Kaspersky Internet Security inclui o Assistente do Privacy Cleaner, que apagado do computador do usuário todas as informações sobre suas ações que poderiam interessar a invasores, inclusive os históricos de sites visitados, os arquivos abertos e os cookies utilizados.

Novos recursos anti-spam:

- A eficiência da filtragem de spam pelo componente Anti-Spam foi melhorada com o uso das tecnologias de servidor Recent Terms (Termos Recentes).

- A utilização dos plugins do Microsoft Outlook, do Microsoft Outlook Express, do The Bat! e do Thunderbird simplifica o processo de configuração do componente Anti-Spam.

- O componente Controle dos Pais revisado permite a restrição efetiva do acesso indesejado das crianças a alguns recursos da Internet.

Novos recursos de proteção para uso da Internet:

- A proteção contra invasores da Internet foi atualizada com a ampliação dos bancos de dados de sites de phishing.

- Foi acrescentada a capacidade de verificação do tráfego do ICQ e do MSN, o que assegura a utilização segura dos mensageiros da Internet.
- A utilização segura de redes sem fio é garantida através da capacidade de varredura de conexões Wi-Fi.

Novos recursos da interface do aplicativo:

- A nova interface do aplicativo reflete a abordagem abrangente à proteção de informações.
- A alta capacidade de informação das caixas de diálogo ajuda o usuário a tomar decisões rapidamente.
- A funcionalidade de registro de estatísticas e criação de relatórios foi ampliada. É possível usar filtros para selecionar dados de relatórios, uma ferramenta sofisticada e flexível insubstituível para os profissionais.

VISÃO GERAL DA PROTEÇÃO DO APLICATIVO

O Kaspersky Internet Security protege seu computador contra ameaças conhecidas e desconhecidas, e contra dados indesejados. Cada tipo de ameaça é processado por um componente específico do aplicativo. Isso torna a configuração flexível, com opções fáceis para todos os componentes, que podem se ajustar às necessidades de um usuário ou da empresa como um todo.

O Kaspersky Internet Security oferece os seguintes recursos de proteção:

- Monitora as atividades do sistema realizadas por aplicativos do usuário, evitando ações perigosas.
- Os componentes de proteção fornecem proteção em tempo real de todas as transferências de dados e caminhos de entrada do computador.
- Os componentes de proteção garantem a segurança do computador contra todos os ataques de rede e de invasores conhecidos no momento durante as conexões com a Internet.
- Os componentes de filtragem removem dados indesejados, economizando tempo, tráfego da Web e dinheiro.

- As tarefas de varredura de vírus são usadas para verificar vírus em arquivos, pastas, unidades ou áreas especificadas individuais, ou em todo o computador. As tarefas de verificação também podem ser configuradas para detectar vulnerabilidades nos aplicativos do usuário instalados.

- O componente de atualização garante que os módulos do aplicativo e os bancos de dados usados para detectar programas maliciosos, ataques de hackers e spams estejam atualizados.

- Assistentes e ferramentas que facilitam a execução de tarefas ocorridas durante o funcionamento do Kaspersky Internet Security.

- Recursos de suporte fornecem informações e assistência para trabalhar com o aplicativo e ampliar seus recursos.

ASSISTENTES E FERRAMENTAS

Assegurar a segurança do computador é uma tarefa complexa, que requer conhecimento sobre os recursos do sistema operacional e os métodos usados para explorar seus pontos fracos. Além disso, o volume e a diversidade de informações sobre a segurança do sistema tornam sua análise e seu processamento difícil.

Para ajudar na execução de tarefas específicas de fornecimento de segurança ao computador, o pacote Kaspersky Internet Security inclui um conjunto de assistentes e ferramentas.

- O Assistente do Analisador de Segurança realiza diagnósticos do computador, pesquisando vulnerabilidades no sistema operacional e nos programas do usuário instalados no computador.

- O Assistente de Configuração de Navegador analisa as configurações do Microsoft Internet Explorer, avaliando-as principalmente do ponto de vista da segurança.

- O Assistente de Restauração do Sistema elimina todos os rastros de ataques de malware no sistema.

- O Assistente do Privacy Cleaner procura e elimina rastros das atividades do usuário no sistema e nas configurações do sistema operacional, evitando a coleta de informações sobre as atividades do usuário.

- O Assistente de Disco de Recuperação restaura a funcionalidade do sistema depois que um ataque de vírus danifica os arquivos do sistema operacional, tornando impossível reiniciar o computador.
- A Análise de Pacotes de Rede intercepta os pacotes de rede e exibe seus detalhes.
- O Monitor de Rede exibe detalhes sobre a atividade de rede no computador.
- O Teclado Virtual evita a interceptação de dados digitados no teclado.

RECURSOS DE SUPORTE

O aplicativo inclui um vários recursos de suporte criados para manter o aplicativo atualizado, ampliar seus recursos e auxiliá-lo na sua utilização.

Kaspersky Security Network

O **Kaspersky Security Network** é um sistema que transfere automaticamente os relatórios sobre ameaças possíveis e detectadas para o banco de dados central da Kaspersky Lab. Esse banco de dados permite à Kaspersky Lab responder mais rapidamente às ameaças mais disseminadas e notificar os usuários sobre surtos de vírus.

Licença

Ao adquirir o Kaspersky Internet Security, você estabelece um contrato de licença com a Kaspersky Lab que regula o uso do aplicativo, o acesso às atualizações do banco de dados do aplicativo e ao Suporte Técnico por um período determinado. Os termos de uso e outras informações necessárias para o funcionamento integral do aplicativo estão incluídos no arquivo da chave de licença.

Usando a função **Licença**, você pode obter informações detalhadas sobre a licença atual, comprar uma nova licença ou renovar a existente.

Suporte

Todos os usuários registrados do Kaspersky Internet Security podem tirar proveito de nosso Serviço de Suporte Técnico. Para ver as informações sobre como obter suporte técnico, use a função **Suporte**.

Seguindo os links correspondentes, você pode acessar o fórum de usuários dos produtos da Kaspersky Lab, enviar um relatório de erros ao Suporte

Técnico ou fazer comentários sobre o aplicativo, preenchendo um formulário online específico.

Você também tem acesso aos serviços online de Suporte Técnico e Gabinete Pessoal do Usuário. Nossa equipe estará sempre pronta a fornecer suporte ao aplicativo por telefone.

ANÁLISE HEURÍSTICA

A análise heurística é usada em alguns componentes de proteção em tempo real, como os componentes Arquivos e memória, E-mail e IM e Tráfego da web, além das varreduras de vírus.

A verificação de objetos usando o método de assinaturas, que utiliza um banco de dados contendo as descrições de todas as ameaças conhecidas, fornece uma resposta definitiva à questão de o objeto verificado ser malicioso e de seu grau de periculosidade. O método heurístico, diferentemente do método de assinaturas, tem como objetivo detectar o comportamento típico de objetos e não seu conteúdo estático, mas não oferece o mesmo nível de precisão em suas conclusões.

A vantagem da análise heurística é que ela detecta malwares não registrados no banco de dados, de forma que não é necessário atualizá-lo antes da varredura. Por isso, as novas ameaças são detectadas antes de serem encontradas pelos analistas de vírus.

Porém, há métodos para contornar a análise heurística. Uma dessas medidas defensivas é congelar a atividade do código malicioso assim que o objeto detecta a verificação heurística.

> Observação
>
> Usar uma combinação de métodos de varredura assegura uma maior segurança.

Ao verificar um objeto, o analisador heurístico emula a execução do objeto em um ambiente virtual seguro fornecido pelo aplicativo. Se for descoberta alguma atividade suspeita enquanto o objeto é executado, ele será considerado malicioso e sua execução no host não será permitida, sendo exibida uma mensagem solicitando instruções do usuário:

- Colocar o objeto em quarentena, o que possibilita a verificação e o processamento posterior da ameaça usando bancos de dados atualizados.

- Excluir o objeto.
- Ignorar (se o usuário tiver certeza de que o objeto não é malicioso).

Para usar os métodos heurísticos, marque a caixa **Usar analisador heurístico** e mova o controle deslizante para uma destas posições: Leve, Média ou Profunda. O nível de detalhamento da varredura permite equilibrar a profundidade e, portanto, a qualidade da varredura de novas ameaças, a carga sobre os recursos do sistema operacional e a duração da varredura. Quando mais alto o nível heurístico definido, mais recursos do sistema serão exigidos pela varredura e mais tempo ela levará.

Aviso!

As novas ameaças detectadas usando a análise heurística são analisadas rapidamente pela Kaspersky Lab e os métodos para desinfectá-las são adicionados às atualizações do banco de dados a cada hora.

Se você atualizar seus bancos de dados regularmente, o nível ideal de proteção do computador será mantido.

REQUISITOS DE HARDWARE E SOFTWARE DO SISTEMA

Para que o computador possa funcionar normalmente, ele deve atender aos seguintes requisitos mínimos:

Requisitos gerais:

- 75 MB de espaço livre no disco rígido.
- CD-ROM (para instalar o aplicativo a partir do CD de instalação).
- Um mouse.
- Microsoft Internet Explorer 5.5 ou superior (para atualização de bancos de dados do aplicativo e módulos do software através da Internet).
- Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (SP2 ou superior), Microsoft Windows XP Professional (SP2 ou superior), Microsoft Windows XP Professional x64 Edition:

- Processador Intel Pentium 300 MHz ou mais rápido (ou equivalente compatível).

- 256 MB de RAM disponível.

Microsoft Windows Vista Starter x32, Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

- Processador Intel Pentium 800 MHz 32 bits (x86) / processador 64 bits (x64) ou mais rápido (ou equivalente compatível).

- 512 MB de RAM disponível.

AMEAÇAS À SEGURANÇA DO COMPUTADOR

Uma ameaça considerável à segurança do computador é imposta pelos aplicativos de ameaça. Além disso, os spams, phishings, ataques de hackers e banners de anúncios de adware também ameaçam o computador. Essas ameaças estão relacionadas com o uso da Internet.

NESTA SEÇÃO:

Aplicativos de ameaça 17

Ameaças da Internet... 39

APLICATIVOS DE AMEAÇA

O Kaspersky Internet Security pode detectar milhares de programas de malware que podem residir em seu computador. Alguns desses programas representam uma ameaça constante ao seu computador, enquanto outros são perigosos apenas em determinadas condições. Depois que o aplicativo detectar um aplicativo de malware, ele o classifica e atribui a ele um nível de perigo (alto ou médio).

Os analistas de vírus da Kaspersky Lab estabelecem duas categorias principais de aplicativos de ameaça: *programas de malware* e *programas potencialmente indesejados*.

Os programas de malware (veja a página 18) são criados para danificar o computador e prejudicar seu usuário: por exemplo, para roubar, bloquear, modificar ou apagar informações, ou para atrapalhar o funcionamento do computador ou da rede de computadores.

Os programas potencialmente indesejados (PUPs) (veja a página 32), diferentemente de outros malwares, não se destinam apenas a causar danos, mas podem ajudar a invadir o sistema de segurança de um computador.

A Enciclopédia de Vírus (http://www.viruslist.com/en/viruses/encyclopedia) contém uma descrição detalhada destes programas.

PROGRAMAS MALICIOSOS

Os **programas maliciosos** ("malware") são criados especificamente para causar danos aos computadores e seus usuários: eles roubam, bloqueiam, modificam ou apagam informações, atrapalham a operação dos computadores ou das redes de computadores.

Os programas de malware são divididos em três subcategorias: *vírus e worms, programas cavalo de Tróia* e *utilitários de malware.*

Os vírus e worms (Viruses_and_Worms) (veja a página 18) podem criar cópias de si mesmos que, por sua vez, se disseminam e se reproduzem novamente. Alguns deles são executados sem o conhecimento ou a participação do usuário, outros requerem ações por parte do usuário para serem executados. Esses programas executam suas ações maliciosas quando executados.

Os cavalos de Tróia (Trojan_programs) (veja a página 22) não criam cópias de si mesmos, ao contrário dos worms e vírus. Eles infectam um computador, por exemplo, por e-mail ou usando um navegador da Web quando o usuário visita um site "infectado". Eles precisam ser iniciados pelo usuário e executam suas ações maliciosas quando executados.

Os utilitários de malware (Malicious_tools) (veja a página 28) são criados especificamente para causar danos. Porém, ao contrário de outros programas de malware, eles não realizam ações maliciosas quando executados e podem ser armazenados e executados seguramente no computador do usuário. Suas funções são usadas por hackers para criar vírus, worms e cavalos de Tróia, para organizar ataques de rede em servidores remotos, invadir computadores ou executar outras ações maliciosas.

VÍRUS E WORMS

Subcategoria: vírus e worms (Viruses_and_Worms)

Nível de gravidade: alto

Os worms e vírus clássicos executam ações não-autorizadas no computador infectado, incluindo sua própria replicação e disseminação.

Vírus clássico

Depois que um vírus clássico se infiltra no sistema, ele infecta um arquivo, se ativa, realiza sua ação maliciosa e depois adiciona cópias de si mesmo a outros arquivos.

Os vírus clássicos se reproduzem nos recursos locais do computador infectado mas não conseguem invadir outros computadores. A distribuição para outros computadores poderá ocorrer somente se o vírus se adicionar a um arquivo armazenado em uma pasta compartilhada ou em um CD, ou se o usuário encaminhar um e-mail com um anexo infectado.

Geralmente, o código de um vírus clássico é especializado na invasão de uma área específica do computador, sistema operacional ou aplicativo. Dependendo do ambiente, há uma distinção entre os *vírus de arquivos, de inicialização, de scripts e de macro*.

Os vírus podem infectar arquivos usando vários métodos. Os vírus de *substituição* gravam seus próprios códigos substituindo o código do arquivo infectado, destruindo o conteúdo original do arquivo. O arquivo infectado pára de funcionar e não pode ser desinfetado. Os vírus *parasitas* modificam arquivos, deixando-os totalmente ou parcialmente operacionais. Os *vírus companheiros* não modificam os arquivos, mas os duplicam; assim, quando o arquivo infectado é aberto, sua duplicata, ou seja, o vírus, é executado. Outros tipos de vírus incluem os *vírus de link*, vírus OBJ que *infectam módulos de objetos*, vírus LIB que *infectam bibliotecas de compiladores* e vírus que *infectam o texto original de programas*.

Worm

Depois de invadir o sistema, um worm de rede, de forma semelhante aos vírus clássicos, é ativado e realiza sua ação maliciosa. O nome worm de rede se deve à sua capacidade de passar secretamente de um computador para outro e de se propagar por meio de vários canais de informações.

Os worms são classificados de acordo com seu método principal de proliferação, conforme listado na tabela a seguir:

Tabela 1. Worms classificados de acordo com seu método de proliferação

TIPO	**NOME**	**DESCRIÇÃO**
IM-Worm	Worms de mensagens instantâneas	Esses worms se propagam através de programas de mensagens instantâneas, como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager e Skype. Geralmente, esses worms usam as listas de contatos para enviar mensagens com um link para um arquivo do worm em um site. Quando um usuário baixa e abre o arquivo, o worm é ativado.
Email-Worm	Worms de e-mail	Os worms de e-mail infectam computadores através de e-mails. A mensagem infectada contém um arquivo anexado com uma cópia de um worm ou um link para um arquivo de worm carregado em um site. Geralmente, esse site foi invadido por hackers ou é o próprio site do hacker. Quando o anexo é aberto, o worm é ativado; ou, quando você clica no link, o arquivo é baixado e aberto e, então, o worm é ativado. Depois, ele continuará a se reproduzir, localizando outros endereços de e-mail e enviando mensagens infectadas a eles.
IRC-Worms	Worms do IRC	Os worms desse tipo entram nos computadores através de canais IRC (Internet Relay Chat), que são usados para se comunicar com outras pessoas através da Internet em tempo real. Esses worms são publicados no canal da Internet, como uma cópia do arquivo do worm ou um link para o arquivo. Quando um usuário baixa e abre o arquivo, o worm é ativado.

TIPO	**NOME**	**DESCRIÇÃO**
Net-Worms	Worms de rede (worms que residem em redes de computadores)	Esses worms são distribuídos através de redes de computadores. Ao contrário dos outros tipos de worms, os worms de rede se propagam sem a participação do usuário. Eles procuram computadores que hospedam programas com vulnerabilidades nas rede local. Isso é feito por meio da transmissão de um pacote de rede (exploração) especial contendo seu código ou uma parte de seu código para cada computador. Se houver um computador vulnerável na rede, o pacote se infiltrará nele. Quando o worm penetra totalmente no computador, ele se torna ativo.
P2P-Worm	Worms de troca de arquivos	Os worms de troca de arquivos se propagam através de redes peer-to-peer para troca de arquivos, como Kazaa, Grokster, EDonkey, FastTrack ou Gnutella. Para usar uma rede de troca de arquivos, o worm faz uma cópia de si mesmo na pasta de troca de arquivos que geralmente se localiza no computador do usuário. A rede de troca de arquivos exibe informações sobre o arquivo, e o usuário pode “localizar” o arquivo infectado na rede como qualquer outro arquivo, baixá-lo e abri-lo. Os worms mais complexos imitam protocolos de rede de uma rede de troca de arquivos específica: eles fornecem respostas positivas a solicitações de pesquisa e oferecem cópias de si mesmos para download.

TIPO	NOME	DESCRIÇÃO
Worm	Outros worms	Outros worms de rede incluem: • Worms que distribuem suas cópias através de recursos de rede. Usando a funcionalidade do sistema operacional, eles passam por pastas de rede disponíveis, conectam-se a computadores na rede global e tentam abrir suas unidades para acesso total. Ao contrário dos worms de rede de computadores, o usuário tem de abrir um arquivo contendo uma cópia do worm para ativá-lo. • Worms que usam outros métodos de propagação não listados aqui, por exemplo, worms que se propagam através de celulares.

CAVALOS DE TRÓIA

Subcategoria: Cavalos de Tróia (Trojan_programs)

Nível de gravidade: alto

Ao contrário de worms e vírus, os cavalos de Tróia não criam cópias de si mesmos. Eles infectam um computador, por exemplo, através de um anexo de e-mail infectado ou por meio de um navegador da Web, quando o usuário visita um site “infectado”. Os cavalos de Tróia são iniciados pelo usuário e começam a realizar suas ações maliciosas ao serem executados.

Os cavalos de Tróia podem executar diversas ações maliciosas. As principais funções dos cavalos de Tróia são bloquear, modificar e apagar dados, além de prejudicar o funcionamento de computadores ou de redes de computadores. Além disso, os cavalos de Tróia podem receber e enviar arquivos, executá-los, exibir mensagens, acessar páginas da Web, baixar e instalar programas e reiniciar o computador infectado.

Freqüentemente, os invasores usam “conjuntos” que consistem em cavalos de Tróia complementares.

Os diferentes tipos de cavalos de Tróia e seus comportamentos estão descritos na tabela a seguir.

Tabela 2. Tipos de cavalos de Tróia de acordo com seu comportamento no computador infectado

TIPO	NOME	DESCRIÇÃO
Trojan-ArcBomb	Cavalos de Tróia – bombas de arquivos comprimidos	Os arquivos comprimidos, quando descompactados, atingem um tamanho que prejudica o funcionamento do computador. Quando você tenta descompactar esse arquivo comprimido, o computador pode começar a funcionar lentamente ou “congelar”, e o disco pode ficar cheio de dados “vazios”. As “bombas de arquivos comprimidos” são especialmente perigosas para servidores de arquivos e e-mail. Se um sistema de processamento automático de informações recebidas for usado no servidor, essa “bomba de arquivos comprimidos” pode interromper o servidor.
Backdoor	Cavalos de Tróia de administração remota	Esses programas são considerados os mais perigosos dentre os cavalos de Tróia. Sua função é semelhante à dos programas de administração remota padrão. Esses programas se instalam sem o conhecimento do usuário e permitem o gerenciamento remoto do computador pelo invasor.

TIPO	NOME	DESCRIÇÃO
Cavalos de Tróia	Cavalos de Tróia	Os cavalos de Tróia incluem os seguintes programas maliciosos: • **cavalos de Tróia clássicos**, que executam apenas as principais funções dos cavalos de Tróia: bloqueiam, modificam ou apagam dados, prejudicando o funcionamento de computadores ou de redes de computadores. Eles não possuem as funções adicionais características dos outros tipos de cavalos de Tróia descritas nesta tabela; • cavalos de Tróia **“com várias finalidades”**, que possuem funções adicionais características de vários tipos de cavalos de Tróia.
Trojan-Ransoms	Cavalos de Tróia que exigem o pagamento de um resgate	Eles "tomam como refém" as informações no computador do usuário e as modificam ou bloqueiam, ou prejudicam o funcionamento do computador, de forma que o usuário não consiga usar os dados. Depois, o invasor pede um resgate ao usuário em troca da promessa de enviar o programa que irá restaurar a funcionalidade do computador.
Cavalos de Tróia de cliques	Cavalos de Tróia de cliques	Esses programas acessam páginas da Web a partir do computador do usuário: eles enviam um comando ao navegador da Web ou substituem os endereços da Web armazenados nos arquivos do sistema. Com esses programas, os invasores organizam ataques de rede ou aumentam o tráfego para sites específicos, aumentando a receita da exibição de banners de anúncios.

TIPO	NOME	DESCRIÇÃO
Trojan-Downloaders	Cavalos de Tróia de download	Esses programas acessam a página da Web do invasor, baixam outros programas de malware e os instalam no computador do usuário. Eles podem armazenar o nome do arquivo de malware disponível para download em seu próprio código ou recebê-lo na página da Web acessada.
Trojan-Droppers	Cavalos de Tróia droppers	Esses programas salvam programas que contêm outros cavalos de Tróia no disco do computador e depois os instalam. Os Trojans-Droppers podem ser usados por invasores de diversas formas: • para instalar programas de malware sem o conhecimento do usuário: os Trojans-Droppers não exibem mensagens ou exibem mensagens falsas, por exemplo, notificando sobre um erro em um arquivo comprimido ou sobre o uso da versão incorreta do sistema operacional; • para impedir que outro programa de malware conhecido seja detectado: nem todos os programas antivírus podem detectar um programa de malware incluído em um Trojan-Dropper.

TIPO	NOME	DESCRIÇÃO
Trojan-Notifiers	Cavalos de Tróia de notificação	Eles notificam o invasor de que o computador infectado está conectado e depois transferem informações sobre o computador para o invasor, incluindo: endereço IP, número de uma porta aberta ou o endereço de e-mail. Eles se comunicam com o invasor através de diversos métodos, como e-mail, FTP ou acessando a página da Web do invasor. Freqüentemente, os Trojans-Notifiers são usados em conjuntos de cavalos de Tróia complementares. Eles notificam o invasor de que outros cavalos de Tróia foram instalados com êxito no computador do usuário.
Cavalos de Tróia de proxy	Cavalos de Tróia de proxy	Eles permitem ao invasor acessar páginas da Web anonimamente usando a identidade do computador do usuário e muitas vezes são usados para enviar spam.
Trojan-PSWs	Cavalos de Tróia que roubam senhas	Esses cavalos de Tróia roubam as contas do usuário, por exemplo, informações de registro de software. Eles encontram informações confidenciais nos arquivos do sistema e no Registro, e as enviam para seus desenvolvedores por e-mail, FTP e acessando o site do invasor. Alguns desses cavalos de Tróia são classificados nos tipos descritos nesta tabela, incluindo Trojan-Bankers, Trojan-IMs e Trojan-GameThieves.

TIPO	NOME	DESCRIÇÃO
Trojan-Spies	Cavalos de Tróia espiões	Esses programas são usados para espionar o usuário: eles coletam informações sobre as ações do usuário no computador. Por exemplo, interceptam os dados digitados pelo usuário no teclado, fazem capturas de tela e coletam listas de aplicativos ativos. Depois de receber essas informações, eles as transferem ao invasor por e-mail, FTP ou acessando o site do invasor.
Trojan-DoS	Cavalos de Tróia que realizam ataques de rede	Nos ataques de negação de serviço (DoS, Denial-of-Service), os cavalos de Tróia enviam numerosas solicitações do computador do usuário para um servidor remoto. Os recursos do servidor serão sobrecarregados com o processamento dessas informações e irão parar de funcionar. Freqüentemente, esses programas são usados para infectar vários computadores, a fim de fazer um ataque combinado ao servidor.
Trojan-IMs	Cavalos de Tróia que roubam dados pessoais de usuários de programas de mensagens instantâneas	Esses programas roubam números e senhas de usuários de programas de mensagens instantâneas, como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager ou Skype. Eles transferem as informações ao invasor por e-mail, FTP ou acessando o site do invasor.
Rootkits	Rootkits	Esses programas escondem outros programas de malware e sua atividade e, assim, estendem a existência desses programas no sistema. Eles ocultam arquivos, processos na memória do computador infectado ou chaves do Registro executadas pelos programas de malware, ou ainda escondem a troca de dados entre aplicativos instalados no computador do usuário e outros computadores na rede.

TIPO	NOME	DESCRIÇÃO
Trojan-SMS	Cavalos de Tróia de mensagens SMS	Esses programas infectam celulares e enviam mensagens SMS para determinados números, pelas quais o usuário do celular infectado é cobrado.
Trojan-GameThieves	Cavalos de Tróia que roubam dados pessoais de usuários de jogos de rede	Esses programas roubam informações de contas de usuários de jogos de rede e as transferem ao invasor por e-mail, FTP ou acessando o site do invasor.
Trojan-Bankers	Cavalos de Tróia que roubam informações de contas bancárias	Esses programas roubam informações de contas bancárias ou informações de contas de débito eletrônica/digital; eles transferem os dados ao invasor por e-mail, FTP ou acessando o site do invasor.
Trojan-Mailfinders	Cavalos de Tróia que coletam endereços de e-mail	Esses programas coletam endereços de e-mail no computador e os transferem para o invasor por e-mail, FTP ou acessando o site do invasor. O invasor pode usar os endereços coletados para enviar spam.

UTILITÁRIOS MALICIOSOS

Subcategoria: utilitários maliciosos (Malicious_tools)

Nível de gravidade: médio

Esses utilitários são projetados especificamente para causar danos. Porém, ao contrário de outros programas de malware, essas ferramentas são usadas principalmente para atacar outros computadores e podem ser armazenadas e executadas no computador do usuário com segurança. Esses programas fornecem funcionalidades para ajudar na criação de vírus, worms e cavalos de Tróia, na organização de ataques de rede em servidores remotos, na invasão de computadores ou em outras ações maliciosas.

Existem diversos tipos de utilitários de malware com funções diferentes, que estão descritos na tabela a seguir.

Tabela 3. Utilitários de malware de acordo com sua função

TIPO	NOME	DESCRIÇÃO
Constructor	Construtores	Os construtores são usados para criar novos vírus, worms e cavalos de Tróia. Alguns construtores possuem uma interface padrão do Windows, que permite ao hacker selecionar o tipo do programa malicioso a ser criado, o método que esse programa usará para resistir ao processo de depuração e outras propriedades semelhantes.
Dos	Ataques de rede	Os programas de negação de serviço (DoS, Denial-of-Service) enviam numerosas solicitações do computador do usuário para um servidor remoto. Os recursos do servidor serão sobrecarregados com o processamento das solicitações e irão parar de funcionar.

TIPO	NOME	DESCRIÇÃO
Exploit	Explorações	Uma exploração é um conjunto de dados ou uma parte de um código de programação que usa as vulnerabilidades de um aplicativo para executar uma ação maliciosa no computador. Por exemplo, as explorações podem gravar ou ler arquivos, ou acessar páginas da Web “infectadas”. As diversas explorações usam as vulnerabilidades dos diferentes aplicativos ou serviços de rede. Uma exploração é transferida através da rede para vários computadores na forma de um pacote de rede, procurando computadores com serviços de rede vulneráveis. Por exemplo, uma exploração em um arquivo DOC procura vulnerabilidades de editores de texto e, quando o usuário abre um arquivo infectado, pode executar as funções programadas pelo invasor. Uma exploração em uma mensagem de e-mail pesquisa vulnerabilidades em programas de e-mail; ela poderá executar suas ações maliciosas assim que o usuário abrir uma mensagem infectada usando esse programa. As explorações também são usadas para distribuir worms de rede (Net-Worm). Exploits-Nukers são pacotes de rede que tornam os computadores inoperantes.
FileCryptors	Codificadores de arquivos	Os codificadores de arquivos criptografam outros programas maliciosos para escondê-los dos aplicativos antivírus.

TIPO	NOME	DESCRIÇÃO
Flooders	Programas usados para inundar redes	Enviam um grande número de mensagens pelos canas de rede, como canais IRC. Entretanto, essa categoria de malware não inclui os programas que inundam o tráfego de e-mail ou os canais de mensagens instantâneas e SMS, que foram classificados separadamente na tabela a seguir (Email-Flooder, IM-Flooder e SMS-Flooder).
HackTools	Ferramentas de hackers	As ferramentas de hackers são usadas para invadir os computadores nos quais elas estão instaladas ou para organizar ataques a outros computadores. Esses ataques incluem: a criação de novas contas de usuário do sistema sem permissão ou a limpeza dos logs do sistema para ocultar traços da presença dos novos usuários no sistema. Eles incluem alguns farejadores que realizam funções maliciosas, por exemplo, a interceptação de senhas. Os farejadores são programas que permitem examinar o tráfego de rede.
not-virus:Hoax	Programas de hoax	Esses programas intimidam o usuário com mensagens semelhantes a vírus: eles podem "detectar" um vírus em um arquivo limpo ou exibir uma mensagem sobre a formatação do disco que não ocorrerá.
Spoofers	Spoofers	Esses programas enviam mensagens e solicitações de rede com o endereço de um remetente falso. Os invasores utilizam spoofers para, por exemplo, fingir ser um remetente legítimo.
VirTools	São ferramentas usadas para criar modificações de programas de malware	Isso é feito para modificar outros programas de malware a fim de escondê-los dos aplicativos antivírus.

TIPO	NOME	DESCRIÇÃO
Email-Flooders	Programas para inundar endereços de e-mail	Esses programas enviam numerosas mensagens para endereços de e-mail (inundando-os). Devido ao grande fluxo de mensagens, os usuários não conseguem visualizar mensagens recebidas que não são spam.
IM-Flooders	Programas usados para inundar programas de mensagens instantâneas	Esses programas enviam numerosas mensagens para usuários de programas de mensagens instantâneas, como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager ou Skype. Devido ao grande fluxo de mensagens, os usuários não conseguem visualizar mensagens recebidas que não são spam.
SMS-Flooders	Programas usados para inundar com mensagens de texto SMS	Esses programas enviam várias mensagens SMS para celulares.

PROGRAMAS POTENCIALMENTE INDESEJADOS

Os **programas potencialmente indesejados**, ao contrário dos programas de malware, não têm como único objetivo causar danos. Porém, eles podem ser usados para violar a segurança do computador.

Os programas potencialmente indesejados incluem adware, pornware e outros *programas potencialmente indesejados*.

Os Adware (veja a página 33) exibem informações publicitárias ao usuário.

Os Pornware (veja a página 33) exibem informações de conteúdo pornográfico ao usuário.

Freqüentemente, outros Riskware (veja a página 34) são programas úteis usados por vários usuários de computador. Porém, se um invasor obtém acesso

a esses programas ou os instala no computador do usuário, ele pode usá-los para violar a segurança do computador.

Os programas potencialmente indesejados são instalados usando um dos seguintes métodos:

- Eles são instalados pelo usuário, individualmente ou juntamente com outro programa. Por exemplo, os desenvolvedores de software incluem programas de adware em programas gratuitos ou shareware.
- Eles também são instalados por invasores. Por exemplo, eles incluem esses programas em pacotes com outros programas de malware, usando as "vulnerabilidades" do navegador da Web ou cavalos de Tróia do tipo downloader ou dropper quando o usuário visita um site "infectado".

ADWARE

Subcategoria: Adware

Nível de gravidade: médio

Os Adware exibem informações publicitárias ao usuário. Eles exibem banners de anúncios na interface de outro programa e redirecionam as pesquisas para sites publicitários. Alguns programas de adware coletam e enviam ao seu desenvolvedor informações de marketing do usuário: por exemplo, quais sites eles visitam ou quais pesquisas eles fazem. Diferentemente dos espiões do tipo cavalo de Tróia, essas informações são transferidas com a permissão do usuário.

PORNWARE

Subcategoria: Pornware

Nível de gravidade: médio

Geralmente, os próprios usuários instalam esses programas ao procurar ou baixar informações pornográficas.

Os invasores podem também instalar esses programas no computador do usuário para exibir anúncios de sites e serviços comerciais de pornografia ao usuário sem sua permissão. Para sua instalação, eles utilizam as

vulnerabilidades do sistema operacional ou do navegador da Web e, em geral, são distribuídos por Trojan-Downloaders e Trojan-Droppers.

Existem três tipos de programas de pornware, conforme classificado na tabela a seguir.

Tabela 4. Tipos de programas de pornware de acordo com suas funções

TIPO	NOME	DESCRIÇÃO
Porn-Dialers	Discadores automáticos	Esses programas contém os números de telefone de serviços pornográficos por telefone e os discam automaticamente. Diferentemente dos discadores do tipo cavalo de Tróia, eles notificam os usuários sobre suas ações.
Porn-Downloaders	Programas para baixar arquivos da Internet	Esses programas baixam pornografia no computador do usuário e, ao contrário dos discadores do tipo cavalo de Tróia, eles notificam os usuários sobre suas ações.
Porn-Tools	Ferramentas	Eles são usados para procurar e exibir pornografia; esse tipo inclui barras de ferramentas do navegador e reprodutores de vídeo especiais.

OUTROS PROGRAMAS DE RISKWARE

Subcategoria: outros programas de riskware

Nível de gravidade: médio

A maioria desses programas é útil e tem uma utilização comum legítima. Eles incluem programas de IRC, discadores, programas de gerenciamento de download de arquivos, monitores de atividade do sistema de computadores, utilitários de gerenciamento de senhas, servidores FTP, HTTP ou Telnet.

Porém, se um invasor obtiver acesso a esses programas ou os instalar no computador do usuário, sua funcionalidade poderá ser usada para violar a segurança do computador.

A tabela lista os programas de riskware de acordo com sua função:

Tabela 5. Tipos de outros riskware de acordo com sua função

TIPO	NOME	DESCRIÇÃO
Client-IRC	Programas de bate-papo pela Internet	Os usuários instalam esses programas para se comunicar através de IRC (Internet Relay Chats).Os invasores os utilizam para disseminar programas de malware.
Dialers	Programas de discagem automática	Esses programas podem estabelecer conexões telefônicas "ocultas" através do modem.
Downloaders	Downloaders	Esses programas podem baixar arquivos de sites secretamente.
Monitores	Monitores	Esses programas monitoram as atividades dos computadores nos quais estão instalados, incluindo o desempenho dos aplicativos e operações de troca de dados com aplicativos em outros computadores.
PSWTools	Ferramentas de recuperação de senhas	Esses programas são usados para visualizar e recuperar senhas esquecidas. Eles são utilizados pelos invasores exatamente da mesma forma quando instalados nos computadores dos usuários.

TIPO	NOME	DESCRIÇÃO
RemoteAdmin	Programas de administração remota	Esses programas são muitas vezes usados pelos administradores de sistemas; eles fornecem acesso a um computador remoto para monitorá-lo e gerenciá-lo. Eles são utilizados pelos invasores exatamente da mesma forma quando instalados nos computadores dos usuários. Os programas riskware de administração remota são diferentes dos programas de administração remota do tipo cavalo de Tróia (ou backdoor). Os cavalos de Tróia podem invadir o sistema e se instalar de forma independente; os programas legítimos não possuem essa funcionalidade.
Server-FTP	Servidores FTP	Esses programas executam as funções de servidores FTP. Os invasores os instalam nos computadores dos usuários para obter acesso remoto através do protocolo FTP.
Server-Proxy	Servidores proxy	Esses programas executam as funções de servidores proxy. Os invasores os instalam nos computadores dos usuários para enviar spam usando a identidade do usuário.
Server-Telnet	Servidores Telnet	Esses programas executam as funções de servidores Telnet. Os invasores os instalam nos computadores dos usuários para obter acesso remoto através do protocolo Telnet.

TIPO	**NOME**	**DESCRIÇÃO**
Server-Web	Servidores Web	Esses programas executam as funções de servidores Web. Os invasores os instalam nos computadores dos usuários para obter acesso remoto através do protocolo HTTP.
RiskTool	Ferramentas do computador local	Essas ferramentas fornecem aos usuários funcionalidades adicionais, sendo usados somente no computador do usuário. Elas permitem que o hacker oculte arquivos, oculte as janelas de aplicativos ativos ou feche processos ativos.
NetTool	Ferramentas de rede	Essas ferramentas permitem que um usuário do computador gerencie remotamente outros computadores na rede: por exemplo, os reinicie, encontre portas abertas ou execute programas instalados nesses computadores.
Client-P2P	Programas peer-to-peer	Esses programas são usados em redes peer-to-peer. Os invasores podem utilizá-los para disseminar programas de malware.
Client-SMTP	Programas SMTP	Esses programas enviam mensagens de e-mail e ocultam essa atividade. Os invasores os instalam nos computadores dos usuários para enviar spam usando as identidades dos usuários.
WebToolbar	Barras de ferramentas da Web	Esses programas adicionam suas próprias barras de ferramentas de pesquisa a outras barras de ferramentas de aplicativos.

TIPO	NOME	DESCRIÇÃO
FraudTool	Programas de fraude	Esses programas se camuflam como outros programas reais. Por exemplo, programas antivírus fraudulentos exibem mensagens sobre a detecção de programas de malware, mas não encontram ou desinfetam nada.

MÉTODOS DE DETECÇÃO DE OBJETOS INFECTADOS, SUSPEITOS E POTENCIALMENTE PERIGOSOS PELO APLICATIVO

O Kaspersky Internet Security detecta programas de malware nos objetos usando dois métodos: o reativo (usando bancos de dados) e o proativo (usando análise heurística).

Os bancos de dados do aplicativo contêm registros usados para identificar centenas de milhares de ameaças conhecidas nos objetos verificados. Esses registros contêm informações sobre as seções de controle do código dos programas de malware e os algoritmos para desinfetar os objetos que contêm esses programas. Os analistas de antivírus da Kaspersky Lab examinam centenas de novos programas de malware diariamente, criam registros que os identificam e os incluem nas atualizações dos arquivos dos bancos de dados.

Se o Kaspersky Internet Security detectar seções de código em um objeto verificado que coincidem totalmente com as seções do código de controle de um programa de malware de acordo com um registro do banco de dados, ele definirá o status do objeto como *infectado*; se houver uma correspondência parcial, o status será definido como *suspeito*.

Usando o método proativo, o aplicativo pode detectar novos programas maliciosos que ainda não estão listados no banco de dados.

O aplicativo detecta objetos que contêm novos programas de malware com base em seus comportamentos. O código de um novo programa de malware pode não coincidir de forma total ou parcial com o de um programa de malware conhecido, mas ele conterá seqüências de comandos características, como a abertura ou a gravação de um arquivo, ou a interceptação de vetores de interrupção. O aplicativo pode determinar, por exemplo, se um arquivo está infectado com um vírus de inicialização desconhecido.

Os objetos detectados usando o método proativo recebem o status de *potencialmente perigosos*.

AMEAÇAS DA INTERNET

O aplicativo da Kaspersky Lab usa tecnologias especiais para evitar as seguintes ameaças ao computador:

- spam ou mensagens recebidas não-solicitadas (consulte a seção "Spam ou e-mails recebidos não-solicitados" na página 39);
- phishing (na página 40);
- ataques de hackers (na página 40);
- exibição de banners (na página 41).

SPAM OU E-MAILS RECEBIDOS NÃO-SOLICITADOS

O aplicativo da Kaspersky Lab protege os usuários contra spam. Os spams são e-mails recebidos não-solicitados e freqüentemente contêm anúncios. Eles representam uma carga adicional na rede e nos servidores do provedor de e-mail. O destinatário paga pelo tráfego criado pelo spam, e os e-mails legítimos trafegam mais lentamente. Por isso, em muitos países o spam é considerado ilegal.

O Kaspersky Internet Security se integra aos programas de e-mail (Microsoft Outlook, Microsoft Outlook Express e The Bat!), e verifica as mensagens recebidas. As mensagens detectadas como spam são processadas de acordo com as ações especificadas pelo usuário: por exemplo, as mensagens podem ser movidas para uma pasta específica ou excluídas.

O Kaspersky Internet Security detecta spam com um alto grau de precisão. Várias tecnologias de filtragem de spam são utilizadas, incluindo: a análise do endereço do remetente e de palavras e frases na linha de assunto da mensagem; ele detecta spam gráfico e utiliza um algoritmo de autotreinamento para detectar spam em função do texto da mensagem.

Os bancos de dados do Anti-Spam contém listas "negra" e "branca" de endereços de remetentes, e listas de palavras e frases relacionadas com diversas categorias de spam, como anúncios, medicina e saúde, e jogos.

PHISHING

O *phishing* é um tipo de atividade fraudulenta na Internet que tem como finalidade "pescar" informações pessoais dos usuários do computador, como números de cartões de créditos e PINs, a fim de roubá-los.

Muitas vezes, o phishing está relacionado a transações bancárias pela Internet. Os invasores criam uma cópia exata do site do banco visado e enviam mensagens aos seus clientes. Os clientes são notificados de que, devido a alterações ou falhas no sistema do banco na Web, as contas dos usuários foram perdidas e que o usuário deve confirmar ou alterar suas informações no site do banco. O usuário acessa o site do invasor e digita seus dados pessoais.

Os bancos de dados de anti-phishing contêm uma lista de sites conhecidos por serem usados para ataques de phishing.

O Kaspersky Internet Security analisa as mensagens recebidas nos programas de e-mail compatíveis (Microsoft Office Outlook e Microsoft Outlook Express) e, se encontrar um link para um site de phishing listado, marca essa mensagem como spam. Se o usuário abrir a mensagem e tentar seguir o link, o aplicativo bloqueará a conexão com o site.

ATAQUES DE HACKERS

Um *ataque de rede* é uma invasão no sistema de um computador remoto a fim de controlá-lo, em geral para causar falhas ou obter acesso a informações protegidas.

Os ataques de rede são ações de invasores (por exemplo, verificações de portas, tentativas de acessar senhas) ou de programas de malware que executam comandos em nome do invasor e, por exemplo, transferem informações para um programa "mestre" remoto. Os programas usados incluem cavalos de Tróia, ataques DoS, scripts maliciosos e determinados tipos de worms de rede.

Os ataques de rede são disseminados em redes locais e globais usando vulnerabilidades dos sistemas operacionais e aplicativos. Eles podem ser transferidos como pacotes de dados IP individuais durante as conexões de rede.

O Kaspersky Internet Security pára os ataques sem interromper as conexões de rede, usando bancos de dados de firewall específicos. Esses bancos de dados contêm registros que identificam pacotes de dados IP característicos enviados por diversos programas de hackers. O aplicativo analisa as conexões de rede e bloqueia os pacotes IP perigosos.

BANNERS

Os *banners de anúncios* são links para o site de um anunciante usualmente exibidos como imagens. A exibição de banners de anúncios em um site não representa qualquer ameaça à segurança do computador, mas ainda é considerada uma interferência no funcionamento normal do computador. Se os banners piscarem na tela, eles afetarão as condições de trabalho e reduzirão a eficiência. O usuário também se distrai com informações irrelevantes e, ao seguir os links dos banners, o tráfego da Internet é aumentado.

Muitas organizações proíbem a exibição de banners de anúncios nas interfaces como parte de suas políticas de segurança de dados.

O Kaspersky Internet Security bloqueia os banners com base na URL do site para o qual há um link no banner de anúncio. Ele utiliza os bancos do dados atualizáveis do Bloqueador de Banner de Anúncio, que contêm uma lista das URLs de redes de banners de anúncios russas e estrangeiras. O aplicativo processa os links da página da Web que está sendo carregada, os compara com a lista de endereços nos bancos de dados e, caso encontre uma correspondência, exclui do site o link para esse endereço e continua carregando a página.

INSTALANDO O APLICATIVO

O aplicativo é instalado no computador de modo interativo, usando o Assistente de Configuração do aplicativo.

Aviso!

É recomendável fechar todos os aplicativos em execução antes de continuar com a instalação.

Para instalar o aplicativo no computador, execute o arquivo de distribuição (com a extensão *.exe).

Observação

A instalação do aplicativo a partir do arquivo de instalação baixado pela Internet é exatamente igual à instalação a partir do CD.

O programa de instalação é implementado como um assistente padrão do Windows. Cada janela contém um conjunto de botões para controlar o processo de instalação. Segue uma breve descrição de suas finalidades:

- **Avançar** – aceita a ação e passa para a próxima etapa do processo de instalação.
- **Voltar** – volta para a etapa anterior do processo de instalação.
- **Cancelar** – cancela a instalação.
- **Concluir** – conclui o procedimento de instalação do aplicativo.

Segue uma discussão detalhada de cada etapa da instalação do pacote.

NESTA SEÇÃO:

Etapa 1. Pesquisando uma versão mais recente do aplicativo 43

Etapa 2. Verificando se o sistema atende aos requisitos de instalação 44

Etapa 3. Janela de boas-vindas do assistente 44

Etapa 4. Exibindo o Contrato de Licença 45

Etapa 5. Selecionando o tipo de instalação.. 45

Etapa 6. Selecionando a pasta de instalação 46

Etapa 7. Selecionando os componentes do aplicativo a serem instalados........ 46

Etapa 8. Procurando outros aplicativos antivírus 47

Etapa 9. Preparação final para a instalação 48

Etapa 10. Concluindo a instalação.. 49

ETAPA 1. PESQUISANDO UMA VERSÃO MAIS RECENTE DO APLICATIVO

Antes de instalar o aplicativo em seu computador, o assistente acessará os servidores de atualização da Kaspersky Lab para verificar se existe uma versão mais recente.

Em caso negativo, o Assistente de Configuração será iniciado e instalará a versão atual.

Se houver uma versão mais recente nos servidores, será perguntado se você deseja baixá-la. Se você cancelar o download, o Assistente de Configuração será iniciado para instalar a versão atual. Se você decidir instalar a versão mais recente, os arquivos de instalação serão baixados para seu computador e o Assistente de Configuração será iniciado automaticamente para instalar a nova versão. Para obter mais detalhes sobre como instalar uma versão mais recente do aplicativo, consulte a documentação da versão.

ETAPA 2. VERIFICANDO SE O SISTEMA ATENDE AOS REQUISITOS DE INSTALAÇÃO

Antes de instalar o aplicativo no seu computador, o assistente irá verificar se o computador atende aos requisitos mínimos (consulte a seção “Requisitos de hardware e software do sistema” na página 15). Ele também irá verificar se você possui os direitos necessários para instalar o software.

Se algum dos requisitos não for atendido, uma notificação correspondente será exibida na tela. É recomendável instalar as atualizações necessárias usando o serviço **Windows Update** e os programas exigidos antes de tentar instalar o Kaspersky Internet Security novamente.

ETAPA 3. JANELA DE BOAS-VINDAS DO ASSISTENTE

Se o seu sistema atender aos requisitos do sistema (consulte a seção “Requisitos de hardware e software do sistema” na página 15) e nenhuma versão mais recente do aplicativo tiver sido encontrada nos servidores de atualização da Kaspersky Lab ou você tiver cancelado a instalação dessa versão, o Assistente de Configuração será iniciado para instalar a versão atual do aplicativo.

A primeira caixa de diálogo do Assistente de Configuração, que indica o início da instalação, será exibida na tela.

Para continuar com a instalação, pressione o botão **Avançar**. Para cancelar a instalação, pressione o botão **Cancelar**.

ETAPA 4. EXIBINDO O CONTRATO DE LICENÇA

A próxima caixa de diálogo do assistente contém o contrato de licença entre você e a Kaspersky Lab. Leia-o atentamente e, se concordar com todos os termos e condições do contrato, selecione **Eu aceito os termos do contrato de licença** e pressione o botão **Avançar**. A instalação continuará.

Para cancelar a instalação, pressione o botão **Cancelar**.

ETAPA 5. SELECIONANDO O TIPO DE INSTALAÇÃO

Nesta etapa, será solicitado que você selecione o tipo de instalação mais adequado a você:

- **Instalação expressa**. Se esta opção for selecionada, o aplicativo inteiro será instalado no seu computador com as configurações de proteção padrão recomendadas pela Kaspersky Lab. Quando a instalação for concluída, o Assistente de Configuração do aplicativo será iniciado.
- **Instalação personalizada**. Ao selecionar esta opção, será solicitado que você escolha os componentes do aplicativo que deseja instalar, especifique a pasta na qual o aplicativo será instalado (consulte a seção "Etapa 6. Selecionando a pasta de instalação" na página 46); ative o aplicativo e o configure usando o Assistente de Configuração do aplicativo.

Se você selecionar a primeira opção, o Assistente de Configuração do aplicativo passará diretamente para a Etapa 8 (consulte a seção "Etapa 8. Procurando outros aplicativos antivírus" na página 47). Caso contrário, a entrada ou confirmação será necessária em cada etapa da instalação.

ETAPA 6. SELECIONANDO A PASTA DE INSTALAÇÃO

Observação

Esta etapa do Assistente de Configuração será executada somente se você selecionar a opção de instalação personalizada (consulte a seção "Etapa 5. Selecionando o tipo de instalação" na página 45).

Nesta etapa, será solicitado que você identifique a pasta do computador na qual o aplicativo será instalado. O caminho padrão é o seguinte:

- **<Unidade>\Arquivos de Programas\Kaspersky Lab\Kaspersky Internet Security 2009** – para sistemas de 32 bits.
- **<Unidade>\Arquivos de Programas (x86)\Kaspersky Lab\Kaspersky Internet Security 2009** – para sistemas de 64 bits.

Você pode especificar uma pasta diferente clicando no botão **Procurar** e selecionando uma pasta na caixa de diálogo de seleção de pastas padrão ou inserindo o caminho da pasta no campo de entrada fornecido.

Aviso!

Observe que, se você inserir manualmente o caminho completo da pasta de instalação, seu tamanho não pode exceder 200 caracteres e o caminho não pode conter caracteres especiais.

Para continuar com a instalação, pressione o botão **Avançar**.

ETAPA 7. SELECIONANDO OS COMPONENTES DO APLICATIVO A SEREM INSTALADOS

Observação: Esta etapa do Assistente de Configuração será executada somente se você selecionar a opção de instalação personalizada (consulte a seção "Etapa 5. Selecionando o tipo de instalação" na página 45).

Durante a instalação personalizada, você deve selecionar os componentes do aplicativo que deseja instalar no computador. Por padrão, todos os componentes do aplicativo são selecionados: componentes de proteção, varredura e atualização.

Para ajudá-lo a decidir quais componentes deseja instalar, existem algumas informações disponíveis sobre cada componente: selecione o componente na lista e leia as informações no campo a seguir. As informações incluem uma breve descrição do componente e o espaço livre no disco rígido necessário para sua instalação.

Para cancelar a instalação de qualquer componente, abra o menu de atalho clicando no ícone ao lado do nome do componente e selecione o item **Componente não estará disponível**. Observe que, se você cancelar a instalação de algum componente, não estará protegido contra diversos programas perigosos.

Para selecionar um componente a ser instalado, abra o menu de atalho clicando no ícone ao lado do nome do componente e selecione **Componente será instalado no disco rígido local**.

Ao concluir a seleção dos componentes a serem instalados, pressione o botão **Avançar**. Para retornar à lista padrão de componentes a serem instalados, pressione o botão **Limpar**.

ETAPA 8. PROCURANDO OUTROS APLICATIVOS ANTIVÍRUS

Nesta etapa, o assistente procura outros programas antivírus, inclusive outros programas da Kaspersky Lab, que podem entrar em conflito com este aplicativo.

Se forem detectados programas antivírus no computador, eles serão listados na tela. Será solicitado que você os desinstale antes de continuar com a instalação.

Você pode escolher se deseja removê-los automaticamente ou manualmente usando os controles localizados abaixo da lista de programas antivírus detectados.

Se a lista de programas antivírus detectada incluir a versão 7.0 do aplicativo da Kaspersky Lab, salve o arquivo da chave do programa ao desinstalá-lo. Você pode usar essa chave para a versão atual do aplicativo. Também é recomendável salvar os objetos armazenados na quarentena e no armazenamento de backup; esses objetos serão movidos automaticamente para

a quarentena da nova versão e você poderá verificá-los novamente após a instalação.

Se você selecionar a remoção automática da versão 7.0, as informações sobre sua ativação serão salvas e reutilizadas na instalação da versão 2009.

> Aviso!
>
> O aplicativo aceita os arquivos de chave das versões 6.0 e 7.0. Não há suporte para as chaves usadas pela versão 5.0 e anteriores.

Para continuar com a instalação, pressione o botão **Avançar**.

ETAPA 9. PREPARAÇÃO FINAL PARA A INSTALAÇÃO

Esta etapa conclui a preparação para a instalação do aplicativo no seu computador.

Durante a instalação inicial e personalizada do aplicativo (consulte a seção "Etapa 5. Selecionando o tipo de instalação" na página 45), é recomendável não desmarcar a caixa **Habilitar Autodefesa antes da instalação**. Se a opção de proteção do módulo estiver habilitada e ocorrer um erro durante a instalação, ele garantirá um procedimento de reversão da instalação correto. Ao repetir a instalação, é recomendável desmarcar essa caixa.

> Observação
>
> Se o aplicativo for instalado remotamente por meio da **Área de Trabalho Remota**, é recomendável desmarcar a caixa **Habilitar Autodefesa antes da instalação**. Se essa caixa estiver marcada, talvez o procedimento de instalação não executado de forma incorreta ou não seja executado.

Para continuar com a instalação, pressione o botão **Avançar**. Será iniciada a cópia dos arquivos de instalação no seu computador.

> Aviso!
>
> Durante o processo de instalação, a conexão atual com a rede será interrompida, caso o pacote do aplicativo inclua componentes que interceptam o tráfego de rede. A maioria das conexões encerradas será restaurada posteriormente.

ETAPA 10. CONCLUINDO A INSTALAÇÃO

A janela **Instalação concluída** contém informações sobre a conclusão da instalação do aplicativo no computador.

Por exemplo, essa janela indicará se é necessário reiniciar o computador para concluir a instalação corretamente. Depois de reiniciar o sistema, o Assistente de Configuração será iniciado automaticamente.

Se não for necessário reiniciar o sistema, pressione o botão **Avançar** para iniciar o Assistente de Configuração do aplicativo.

INTERFACE DO APLICATIVO

O aplicativo possui uma interface simples e fácil de usar. Este capítulo aborda detalhadamente seus recursos básicos.

Além da interface principal do aplicativo, existem plugins para o Microsoft Outlook, o The Bat! e o Microsoft Windows Explorer. Esses plugins ampliam a funcionalidade desses programas, pois permitem que os componentes do Kaspersky Internet Security sejam gerenciados e configurados a partir da interface dos programas.

NESTA SEÇÃO:

Ícone da área de notificação 50

Menu de atalho 51

Janela principal do aplicativo 53

Notificações 56

Janela de configurações do aplicativo 56

ÍCONE DA ÁREA DE NOTIFICAÇÃO

Logo depois da instalação, o ícone do aplicativo aparecerá na área de notificação da barra de tarefas do Microsoft Windows.

Esse ícone indica a operação atual do aplicativo. Ele também reflete o status da proteção e mostra várias funções básicas executadas pelo programa.

Se o ícone está ativo (colorido), a proteção completa aplicativo o alguns de seus componentes estão em execução. Se o ícone está inativo (preto e branco), todos os componentes de proteção estão desabilitados.

O ícone do aplicativo muda de acordo com a operação em execução:

– verificação de e-mail.

– atualização de bancos de dados e módulos do aplicativo.

– é necessário reiniciar o computador para aplicar as atualizações.

– erro em algum componente do Kaspersky Internet Security.

O ícone também dá acesso às funções básicas da interface do aplicativo, incluindo o menu de atalho (consulte a seção "Menu de atalho" na página 51) e janela principal do aplicativo (consulte a seção "Janela principal do aplicativo" na página 53).

Para abrir o menu de atalho, clique com o botão direito do mouse no ícone do aplicativo.

Para abrir a janela principal do aplicativo, clique duas vezes no ícone do aplicativo. A janela principal sempre é aberta na seção **Proteção**.

Se houver notícias da Kaspersky Lab disponíveis, o ícone de notícias aparecerá na área de notificação da barra de tarefas . Clique duas vezes no ícone para exibir as notícias em uma nova janela.

MENU DE ATALHO

Você pode executar as tarefas de proteção básicas a partir do menu de contexto, que contém os seguintes itens:

- **Atualização** - inicia as atualizações do banco de dados e dos módulos do aplicativo e instala as atualizações no computador.
- **Verificação completa do computador** – inicia uma verificação completa de objetos perigosos no computador. Os objetos que residem em todas as unidades, incluindo mídias de armazenamento removíveis, serão verificados.
- **Verificação de vírus** – seleciona objetos e inicia uma verificação de vírus. A lista padrão dessa varredura contém vários objetos, como a pasta **Meus documentos** e os arquivos comprimidos de e-mail. Você

pode selecionar outros objetos a serem verificados e adicioná-los à lista.

- **Monitor de Rede** – exibe a lista de conexões de rede estabelecidas, portas abertas e o tráfego de rede.
- **Teclado Virtual** – alterna para o teclado virtual.
- **Kaspersky Internet Security** – abre a janela principal do aplicativo (consulte a seção "Janela principal do aplicativo" na página 53).
- **Configurações** – exibe e modifica as configurações do aplicativo.
- **Ativar** – ativa o programa. Para se tornar um usuário registrado, é necessário ativar o aplicativo. Este item de menu estará disponível somente se o aplicativo não tiver sido ativado.
- **Sobre** – exibe informações sobre o aplicativo.
- **Pausar proteção / Continuar proteção** – habilita ou desabilita temporariamente os componentes de proteção em tempo real. Essa opção do menu não afeta a execução das atualizações do aplicativo ou da tarefa de varredura de vírus.
- **Bloqueio do tráfego de rede** – bloqueia temporariamente todas as conexões de rede do computador. Se desejar permitir a interação entre o computador e a rede, clique novamente nesse item no menu de contexto.

- **Sair** – fecha o aplicativo e o descarrega da memória do computador.

Atualização
Verificação completa do computador
Verificação de vírus...

Monitor de rede
Teclado virtual

Kaspersky Internet Security
Configurações
Sobre

Pausar proteção...
Bloquear tráfego de rede

Sair
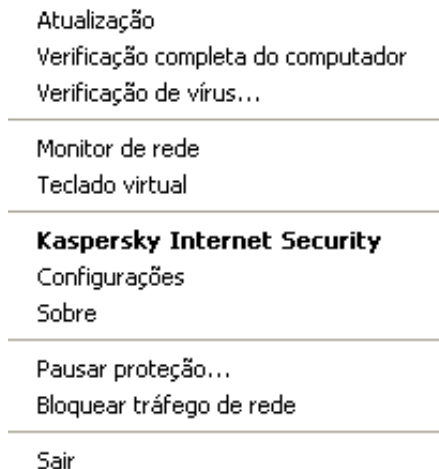
Figura 1: Menu de atalho

Se uma tarefa de varredura de vírus estiver em execução quando você abrir o menu de atalho, o nome e o status de andamento da tarefa (porcentagem de conclusão) serão exibidos no menu de atalho. Ao selecionar a tarefa, você abrirá a janela principal do aplicativo, que contém um relatório sobre os resultados atuais da execução da tarefa.

JANELA PRINCIPAL DO APLICATIVO

A janela principal do aplicativo pode ser dividida em três partes:

- A parte superior da janela indica o status de proteção atual do computador.

Figura 2: Status atual da proteção do computador

Três status de proteção são possíveis: cada um deles é indicado por uma cor, de forma semelhante às luzes de sinalização de tráfego. A cor

verde indica que a proteção do computador está no nível correto; as cores amarela e vermelha indicam ameaças de segurança na configuração do sistema ou na operação do aplicativo. Além dos programas de malware, as ameaças incluem bancos de dados do aplicativo obsoletos, componentes de proteção desabilitados e a seleção dos níveis mínimos de configuração da proteção.

As ameaças de segurança devem ser eliminadas assim que aparecerem. Para obter informações detalhadas sobre elas e para eliminá-las rapidamente, use o link **Reparar agora** (veja a figura acima).

- Na parte esquerda da janela, a barra de navegação fornece acesso rápido às funções do aplicativo, incluindo as tarefas de varredura antivírus e de atualização.

Figura 3: Parte esquerda da janela principal

- A parte direita da janela contém informações sobre a função do aplicativo selecionada à esquerda, sendo usada para definir as configurações dessas funções, além de exibir ferramentas para executar tarefas de varredura antivírus, download de atualizações, etc.

Figura 4: Parte informativa da janela principal

Você também pode usar estes botões:

- **Configurações** – para abrir a janela de configurações do aplicativo.
- **Ajuda** – para abrir o sistema de Ajuda do aplicativo.
- **Detectado** – para abrir a lista de objetos nocivos detectados por qualquer componente ou tarefa de varredura antivírus, e exibir estatísticas detalhadas do funcionamento do aplicativo.
- **Relatórios** – para abrir a lista de eventos ocorridos durante a operação do aplicativo.
- **Suporte** – para exibir informações sobre o sistema e links para os recursos de informação da Kaspersky Lab, incluindo o site do Serviço de Suporte Técnico e o fórum.

> Observação
>
> Você pode alterar a aparência do aplicativo criando e usando seus próprios elementos gráficos e esquemas de cores.

NOTIFICAÇÕES

Se ocorrerem eventos durante a operação do aplicativo, notificações específicas serão exibidas na tela como mensagens pop-up acima do ícone do aplicativo na barra de tarefas do Microsoft Windows.

Dependendo do grau de importância do evento para a segurança do computador, você poderá receber os seguintes tipos de notificações:

- **Alerta**. Ocorreu um evento crítico; por exemplo, foi detectado um vírus ou uma atividade perigosa no seu sistema. Você deve decidir imediatamente como lidar com essa ameaça. Esse tipo de notificação aparece em vermelho.
- **Aviso**! Ocorreu um evento possivelmente perigoso. Por exemplo, foram detectados arquivos possivelmente infectados ou uma atividade suspeita no sistema. Instrua o programa de acordo com o nível de periculosidade que você atribui ao evento. Esse tipo de notificação aparece em amarelo.
- **Observação**: Esta notificação fornece informações sobre eventos não-críticos. Esse tipo inclui, por exemplo, notificações relacionadas à operação do componente **Filtragem de Conteúdo**. As notificações informativas aparecem em verde.

JANELA DE CONFIGURAÇÕES DO APLICATIVO

A janela de configurações do aplicativo pode ser aberta a partir da janela principal do aplicativo (consulte a seção "Janela principal do aplicativo" na página 53) ou do menu de atalho (consulte a seção "Menu de atalho" na página 51). Para abrir essa janela, clique no link **Configurações** na parte superior da janela principal do aplicativo ou selecione a opção apropriada no menu de atalho do aplicativo.

A janela de configurações consiste em duas partes:

- à esquerda da janela, você tem acesso aos componentes do aplicativo, tarefas de varredura de vírus e tarefas de atualização;

- à direita da janela, existe uma lista de configurações do componente ou tarefa selecionado à esquerda.

INTRODUÇÃO

Ao criar o Kaspersky Internet Security, um dos principais objetivos da Kaspersky Lab foi fornecer uma configuração ideal para todas as opções do aplicativo. Isso permite que até mesmo um usuário de computador iniciante proteja seu computador imediatamente após a instalação, sem precisar gastar horas alterando as configurações.

Para sua conveniência, os primeiros estágios de configuração foram reunidos em um Assistente de Configuração Inicial unificado que é iniciado assim que o programa é instalado. Seguindo as instruções do assistente, você pode ativar o aplicativo, definir as configurações das atualizações, restringir o acesso ao programa por senha e executar outras configurações.

Seu computador pode estar infectado com malware antes de o aplicativo ser instalado. Para detectar programas de malware existentes, execute uma varredura do computador (consulte a seção "Verificando vírus no computador" na página 61).

As configurações do computador podem ter sido corrompidas por uma infecção por malware ou por falhas do sistema. Execute o Assistente de Análise de Segurança para localizar as vulnerabilidades do software instalado e as anomalias das configurações do sistema.

Provavelmente, os bancos de dados do aplicativo fornecidos com o pacote de instalação estarão desatualizados. Inicie a atualização do aplicativo (consulte a página 60), caso ela não tenha sido executada pelo Assistente de Configuração ou automaticamente, logo após a instalação do aplicativo.

O componente Anti-Spam incluído na estrutura do aplicativo usa um algoritmo de autotreinamento para detectar mensagens indesejadas. Inicie o Assistente de Treinamento do Anti-Spam para configurar o componente para trabalhar com suas mensagens.

Depois de concluir as ações nesta seção, o aplicativo estará pronto para proteger seu computador. Para avaliar a proteção do computador, use o Assistente de Gerenciamento de Segurança (consulte a seção "Gerenciamento de segurança" na página 67).

NESTA SEÇÃO:

Selecionando o tipo de rede 59

Atualizando o aplicativo 60

Análise de segurança 60

Verificando vírus no computador 61

Gerenciando a licença 62

Assinatura para renovação automática da licença 63

Participando do Kaspersky Security Network 65

Gerenciamento de segurança 67

Pausando a proteção 69

SELECIONANDO O TIPO DE REDE

Depois de concluir a instalação, o componente Firewall analisa as conexões de rede ativas do computador. Será atribuído um status a cada conexão de rede, determinando as atividades de rede permitidas.

Se você selecionou o modo interativo do Kaspersky Internet Security, será exibida uma notificação sempre que uma conexão de rede for estabelecida. Você pode selecionar o status das novas redes na janela de notificação:

- **Rede pública** – o acesso externo ao computador é bloqueado, e o acesso a pastas públicas e impressoras também é bloqueado. Esse status é recomendável para conexões com a Internet.
- **Rede local** – o acesso a pastas públicas e impressoras de rede é permitido. É recomendável atribuir esse status às redes locais protegidas, por exemplo, uma rede corporativa.
- **Rede confiável** – todas as atividades são permitidas. É recomendável atribuir esse status somente às áreas absolutamente seguras.

O Kaspersky Internet Security inclui um conjunto de regras para gerenciar as atividades de rede de cada status de rede. Subseqüentemente, você pode alterar o status de rede especificado para cada conexão, assim que ela for detectada pela primeira vez.

ATUALIZANDO O APLICATIVO

Aviso!

É necessário ter uma conexão com a Internet para atualizar o Kaspersky Internet Security.

O Kaspersky Internet Security inclui bancos de dados que contêm assinaturas de ameaças, exemplos de frases características de spam e descrições de ataques de rede. Porém, no momento da instalação do aplicativo, talvez os bancos de dados já estejam obsoletos, pois a Kaspersky Lab atualiza os bancos de dados e os módulos do aplicativo regularmente.

Você pode especificar o modo como a tarefa de atualização será iniciada no Assistente de Configuração do aplicativo. Por padrão, o Kaspersky Internet Security verifica automaticamente as atualizações nos servidores de atualização da Kaspersky Lab. Se o servidor contiver novas atualizações, o aplicativo as baixará e instalará no modo silencioso.

Para manter a proteção de seu computador atualizada, é recomendável atualizar o Kaspersky Internet Security imediatamente após a instalação.

- *Para atualizar o Kaspersky Internet Security manualmente,*

  1. Abra a janela principal do aplicativo.

  2. Selecione a seção **Atualização** à esquerda da janela.

  3. Pressione o botão **Iniciar atualização**.

ANÁLISE DE SEGURANÇA

O sistema operacional do seu computador pode ser danificado por falhas do sistema e pelas atividades de programas de malware. Além disso, os aplicativos do usuário instalados podem ter vulnerabilidades exploradas pelos invasores para causar danos ao seu computador.

Para detectar e eliminar esses problemas de segurança, é recomendável executar o *Assistente do Analisador de Segurança* imediatamente depois de instalar o aplicativo. O Assistente do Analisador de Segurança procura vulnerabilidades nos aplicativos instalados, além de danos e anomalias nas configurações do sistema operacional e do navegador.

- *Para iniciar o assistente:*

1. Abra a janela principal do aplicativo.

2. À esquerda da janela, selecione **Segurança do Sistema**.

3. Inicie a tarefa do **Analisador de Segurança**.

VERIFICANDO VÍRUS NO COMPUTADOR

Os desenvolvedores de malware se empenham ao máximo para ocultar as ações de seus programas. Por isso, talvez você não perceba a presença de programas de malware no seu computador.

Assim que é instalado no computador, o Kaspersky Internet Security executa automaticamente uma **Verificação rápida**. Essa tarefa procura e neutraliza programas perigosos nos objetos carregados na inicialização do sistema operacional.

Os especialistas da Kaspersky Lab também recomendam que você execute a tarefa de **Verificação completa**.

- *Para iniciar/parar uma tarefa de varredura de vírus:*

1. Abra a janela principal do aplicativo.

2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).

3. Pressione o botão **Iniciar verificação** para iniciar a varredura. Se precisar interromper a execução da tarefa, pressione o botão **Parar verificação** enquanto a tarefa estiver em andamento.

GERENCIANDO A LICENÇA

É necessária uma chave de licença para o funcionamento do aplicativo. Uma chave será fornecida quando você adquirir o programa. Com ela, você tem o direito de usar o programa a partir do dia da compra e da instalação da chave.

Sem uma chave de licença, a menos que uma versão de teste do aplicativo tenha sido ativada, o aplicativo será executado no modo que permite apenas uma atualização. O aplicativo não baixará novas atualizações.

Se uma versão de teste do programa tiver sido ativada, depois de expirado o período de teste, ele não será executado.

Quando a chave de licença expirar, o programa continuará funcionando, exceto pelo fato de você não poder atualizar os bancos de dados. Como antes, você poderá verificar seu computador quanto à presença de vírus e usar os componentes de proteção, mas apenas com os bancos de dados que você tinha antes de a licença expirar. Não podemos garantir que você estará protegido contra os vírus que surgirem depois que a licença do programa expirar.

Para proteger seu computador da infecção por novos vírus, é recomendável renovar a chave do aplicativo. Duas semanas antes da expiração da chave do aplicativo, você será notificado. Durante algum tempo, uma mensagem correspondente será exibida sempre que o aplicativo for iniciado.

As informações sobre a chave atual são mostradas em **Licença**, na janela principal do aplicativo: ID da chave, tipo (comercial, comercial com assinatura, comercial com assinatura de proteção, experimental, beta), número de hosts nos quais esta chave pode ser instalada, data de expiração da chave e número de dias restantes até a expiração. As informações sobre a expiração da chave não serão exibidas se houver uma licença comercial com assinatura ou licença comercial com assinatura de proteção instalada (consulte a seção "Assinatura para a renovação automática da licença" na página 63).

Para exibir os termos do contrato de licença do aplicativo, clique no botão **Exibir Contrato de Licença do Usuário Final**. Para remover uma chave da lista, clique no botão **Excluir**.

Para adquirir ou renovar uma chave:

1. Adquira uma nova chave. Para fazê-lo, use o botão **Comprar licença** (caso o aplicativo não tenha sido ativado) ou **Renovar licença**. A página da Web que é aberta contém todas as informações sobre a compra de uma chave na loja virtual ou através dos parceiros

corporativos da Kaspersky Lab. Se você comprar on-line, um arquivo de chave ou um código de ativação será enviado por e-mail para o endereço especificado no formulário do pedido assim que o pagamento for efetuado.

2. Instale a chave. Para fazê-lo, use o botão **Instalar chave** na seção **Licença** da janela principal do aplicativo ou use o comando **Ativação** no menu principal do aplicativo. O Assistente de Ativação será iniciado.

Observação: Periodicamente, a Kaspersky Lab lança ofertas de extensões de licença de nossos produtos. Verifique as ofertas no site da Kaspersky Lab, em **Produtos → Vendas e ofertas especiais**.

ASSINATURA PARA RENOVAÇÃO AUTOMÁTICA DA LICENÇA

Ao licenciar usando uma assinatura, o aplicativo entrará em contato automaticamente com o servidor de ativação em intervalos específicos para manter a validade de sua licença durante todo o período da assinatura.

Se a chave atual tiver expirado, o Kaspersky Internet Security verificará a disponibilidade de uma chave atualizada no servidor usando o modo de segundo plano e, ao encontrá-la, ela será baixada e instalada em substituição à chave anterior. Dessa forma, a licença será renovada sem o seu envolvimento no processo. Se o período em que o próprio aplicativo renova a licença também tiver expirado, a licença poderá ser renovada manualmente. Durante o período em que a renovação manual da licença é permitida, a funcionalidade do aplicativo será mantida. Após esse período, se a licença não tiver sido renovada, as atualizações dos bancos de dados não serão carregadas (para a licença comercial com assinatura) e a proteção do computador não será mais assegurada (para a licença comercial com assinatura de proteção). Para rejeitar a assinatura para renovação automática da licença, entre em contato com a loja virtual em que você adquiriu o aplicativo.

Aviso!

Se, no momento da ativação, o aplicativo já estiver ativado usando uma chave comercial, essa chave será substituída por uma chave de assinatura (uma chave de assinatura de proteção). Se você desejar usar a chave comercial novamente, exclua a chave de assinatura e ative o aplicativo novamente com o código de ativação usado ao obter a chave comercial.

A condição da assinatura é caracterizada da seguinte maneira:

1. *Corrompido*. Sua solicitação de ativação da assinatura ainda não foi processada (é necessário um tempo para o processamento da solicitação no servidor). O Kaspersky Internet Security trabalha no modo de funcionamento completo. Se, após um determinado período, a solicitação da assinatura ainda não tiver sido processada, você receberá uma notificação. Nesse caso, os bancos de dados do aplicativo não serão mais atualizados (para a licença comercial com assinatura) e a proteção do computador não será executada (para a licença comercial com assinatura de proteção).

2. *Ativação*. A assinatura para renovação automática da licença foi ativada por um período ilimitado (sem uma data especificada) ou por um período determinado (a data de expiração da assinatura foi especificada).

3. *Renovada*. A assinatura foi renovada automaticamente ou manualmente por um período ilimitado (sem uma data especificada) ou por um período determinado (a data de expiração da assinatura foi especificada).

4. *Erro*. Ocorreu um erro na renovação da assinatura.

5. *Expirada*. O período da assinatura acabou. Você pode usar outro código de ativação ou renovar sua assinatura, entrando em contato com a loja virtual na qual o aplicativo foi adquirido.

6. *Cancelamento da assinatura*. Você cancelou a assinatura para renovação automática da licença.

7. *Atualização necessária*. Por algum motivo, a chave para renovação da assinatura não foi recebida a tempo. Use a opção **Renovar o status da assinatura** para renovar a assinatura.

Para a licença comercial com assinatura de proteção, a assinatura se caracteriza por dois status adicionais:

- *Suspensa*. A assinatura para a renovação automática da licença está suspensa (data de expiração da assinatura: data de suspensão da validade da assinatura).

- *Reiniciada*. A assinatura para renovação automática da licença foi reiniciada (a data de expiração da assinatura não é limitada).

Se o período de validade da assinatura tiver acabado, assim como o período adicional em que a licença pode ser renovada (status da assinatura – *Expirada*) o aplicativo o notificará e não tentará mais obter uma chave atualizada do servidor. Para a licença comercial com assinatura, a funcionalidade do aplicativo será mantida, exceto pelo recurso de atualização dos bancos de dados do aplicativo. Para a licença comercial com assinatura de proteção, os bancos de dados não serão atualizados e a proteção do computador não será executada.

Se, por algum motivo, a licença não foi renovada (status da assinatura – *Atualização necessária*) a tempo (por exemplo, se o computador estava desligado durante o período em que a renovação da licença estava disponível), você poderá renová-la manualmente. Para fazê-lo, é possível usar o botão **Renovar o status da assinatura**. Até o momento da renovação da assinatura, o Kaspersky Internet Security interrompe a atualização dos bancos de dados do aplicativo (para a licença comercial com assinatura) e pára de executar a proteção do computador (para a licença comercial com assinatura de proteção).

Enquanto estiver usando a assinatura, você não poderá instalar chaves de outro tipo ou usar outro código de ativação para renovar a licença. É possível usar outro código de ativação somente depois de encerrado o período da assinatura (status da assinatura – *Expirada*).

Aviso!

Ao usar a assinatura para renovação automática da licença, se você reinstalar o aplicativo no computador, será necessário ativar o produto manualmente novamente usando o código de ativação obtido ao adquirir o aplicativo.

PARTICIPANDO DO KASPERSKY SECURITY NETWORK

Um grande número de novas ameaças aparece diariamente em todo o mundo. Para facilitar a coleta de estatísticas sobre os novos tipos de ameaça, suas origens e como eliminá-las, a Kaspersky Lab o convida a usar o serviço Kaspersky Security Network.

Ao usar o Kaspersky Security Network, as seguintes informações são enviadas para a Kaspersky Lab:

- Um identificador exclusivo atribuído ao seu computador pelo aplicativo. Esse identificador caracteriza as configurações de hardware do computador e não contém qualquer outra informação.

- As informações sobre as ameaças detectadas pelo aplicativo. A estrutura e o conteúdo das informações dependem do tipo de ameaça detectada.
- Informações do sistema: a versão do sistema operacional, os service packs instalados, os serviços e drivers para download, as versões do navegador e do programa de e-mail, as extensões do navegador, o número da versão instalada do Kaspersky Internet Security.

O Kaspersky Security Network também coleta também estatísticas ampliadas, incluindo informações sobre:

- arquivos executáveis e aplicativos assinados baixados no seu computador;
- aplicativos em execução no computador.

Essas informações estatísticas são enviadas ao concluir a atualização do aplicativo.

> Aviso!
>
> A Kaspersky Lab garante que nenhuma coleta e distribuição de dados pessoais do usuário será realizada pelo Kaspersky Security Network.

► Para configurar o envio de estatísticas:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Feedback** à esquerda da janela.
3. Marque a caixa **Eu concordo em participar do programa Kaspersky Security Network** para confirmar sua participação no Kaspersky Security Network. Marque a caixa **Eu concordo em enviar estatísticas ampliadas dentro da estrutura do Kaspersky Security Network** para confirmar seu consentimento em enviar as estatísticas ampliadas.

GERENCIAMENTO DE SEGURANÇA

Os problemas na proteção do computador são indicados na janela principal do aplicativo, através da alteração da cor do ícone de status de proteção e do painel em que esse ícone se localiza. Quando houver problemas no sistema de proteção, será recomendado que você os corrija imediatamente.

Figura 5: Status atual da proteção do computador

Você pode visualizar a lista de problemas atuais, suas descrições e as possíveis soluções na guia **Status** (veja a figura abaixo) que é aberta ao clicar no link **Reparar agora** (veja a figura acima).
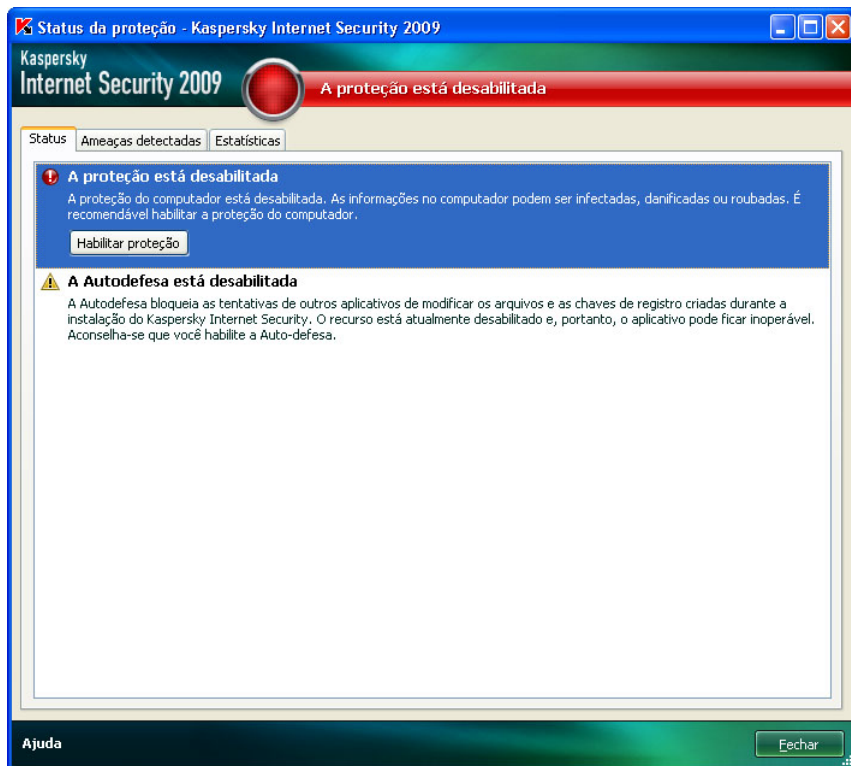
Figura 6: Resolvendo de problemas de segurança

A guia mostra a lista de problemas atuais. Os problemas são listados em ordem de importância: primeiro, os problemas mais críticos, marcados com o ícone de status vermelho; em segundo lugar, os problemas menos importantes, marcados com o ícone de status amarelo e, por último, as mensagens informativas, marcadas com o ícone verde. É fornecida uma descrição detalhada de cada problema, e as seguintes ações estão disponíveis:

- *Eliminar imediatamente*. Usando os botões correspondentes, você pode corrigir o problema, que é a ação recomendada.
- *Adiar a eliminação*. Se, por algum motivo, não for possível eliminar o problema imediatamente, você poderá adiar essa ação e voltar a ela

posteriormente. Para adiar a eliminação, use o botão **Ocultar mensagem**.

No caso de problemas graves, essa opção não estará disponível. Esses problemas incluem, por exemplo, objetos maliciosos detectados e que não foram desinfetados, travamento de um ou de vários componentes ou corrupção dos arquivos do aplicativo.

Para que as mensagens ocultas reapareçam na lista geral, marque a caixa **Mostrar mensagens ocultas**.

PAUSANDO A PROTEÇÃO

Pausar a proteção significa desabilitar temporariamente todos os componentes de proteção por um determinado período.

- *Para pausar a proteção do computador:*

1. Selecione **Pausar Proteção** no ***menu de atalho*** do aplicativo (consulte a seção "Menu de atalho" na página 51).

2. Na janela **Pausar proteção** que será aberta, selecione o período no qual você deseja que a proteção seja pausada:

   - **Em <intervalo de tempo>** – a proteção será habilitada após este período. Use o menu suspenso para selecionar o valor do intervalo de tempo.

   - **Continuar após a reinicialização** – a proteção será habilitada depois da reinicialização do sistema, desde que o aplicativo também esteja configurado para ser executado ao reiniciar o computador.

   - **Continuar manualmente** – a proteção será reiniciada somente depois de você executá-la manualmente. Para habilitar a proteção, selecione Continuar proteção no menu de atalho do aplicativo.

Ao desabilitar a proteção temporariamente, todos os componentes de proteção serão pausados. Isso é indicado por:

- Nomes inativos (cinza) dos componentes desabilitados na seção **Proteção** da janela principal.

- Ícone do aplicativo inativo (cinza) (consulte a seção "Ícone da área de notificação" na página 50) no painel do sistema.
- A cor vermelha do ícone de status e do painel da janela principal do aplicativo.

Se houver conexões de rede estabelecidas no momento em que a proteção é pausada, é exibida uma notificação sobre o encerramento dessas conexões.

VALIDANDO AS CONFIGURAÇÕES DO APLICATIVO

Depois que o aplicativo for instalado e configurado, você deverá verificar se ele está configurado corretamente usando um “vírus” de teste e suas modificações. É necessário realizar um teste separado para cada componente/protocolo de proteção.

NESTA SEÇÃO:

Testar o "vírus" da EICAR e suas modificações 71

Testando a proteção do tráfego HTTP 75

Testando a proteção do tráfego SMTP 76

Validando as configurações de Arquivos e memória 76

Validando as configurações da tarefa de varredura de vírus 77

Validando as configurações do Anti-Spam 78

TESTAR O "VÍRUS" DA EICAR E SUAS MODIFICAÇÕES

Este "vírus" de teste foi especialmente desenvolvido pelo eicar (Instituto Europeu para Pesquisa de Antivírus de Computador) para testar produtos antivírus.

O "vírus" de teste NÃO É UM VÍRUS porque não contém nenhum código que possa danificar seu computador. Entretanto, a maioria dos produtos antivírus de vários fabricantes identificam esse arquivo como um vírus.

> Aviso!
>
> Nunca use vírus reais para testar o funcionamento de um produto antivírus.

Você pode baixar o "vírus" de teste do site oficial da organização **EICAR** em: http://www.eicar.org/anti_virus_test_file.htm.

> Observação
>
> Antes de baixar o arquivo, desabilite a proteção antivírus do computador; caso contrário, o aplicativo identificará e processará o arquivo *anti_virus_test_file.htm* como um objeto infectado transferido através do protocolo HTTP.
>
> Não esqueça de habilitar a proteção antivírus imediatamente depois de baixar o "vírus" de teste.

O aplicativo identifica os arquivos baixados do site da **EICAR** como um objeto infectado que contém um vírus que **não pode ser desinfetado** e executa as ações especificadas para esse objeto.

Também é possível modificar o “vírus” de teste padrão para verificar o funcionamento do aplicativo com relação a outros tipos de arquivos. Para modificar o “vírus”, altere o conteúdo do “vírus” padrão, adicionando um dos prefixos a ele (veja a tabela a seguir). Para criar os arquivos de “vírus” modificados, você pode usar qualquer editor de texto ou de hipertexto, por exemplo, o **Bloco de Notas da Microsoft**, o **UltraEdit32**, etc.

> Aviso!
>
> Você poderá testar se o aplicativo antivírus funciona corretamente usando o "vírus" da EICAR modificado somente se seus bancos de dados de antivírus foram atualizados pela última vez em ou depois de 24 de outubro de 2003 (atualizações cumulativas de outubro de 2003).

A primeira coluna da tabela a seguir contém os prefixos que devem ser adicionados ao início do texto do “vírus” padrão. A segunda coluna lista os status possíveis que o aplicativo pode atribuir ao objeto com base nos resultados da varredura. A terceira coluna indica como o aplicativo processa os objetos com o status especificado. As ações reais executadas com os objetos são determinadas pelas configurações do aplicativo.

Depois de ter adicionado o prefixo ao "vírus" de teste, salve o novo arquivo com um nome diferente, por exemplo: *eicar_dele.com*. Atribua nomes semelhantes a todos os "vírus" modificados.

Tabela 6. Modificações do "vírus" de teste

Prefixo	**Status do objeto**	**Informação sobre o processamento do objeto**
Sem prefixo, vírus de teste padrão	**Infectado**. O objeto infectado contém o código de um vírus conhecido. A desinfecção não é possível.	O aplicativo identifica o objeto como um vírus que não pode ser desinfetado. Ocorre um erro ao tentar desinfetar o objeto; a ação atribuída a ser realizada com objetos que não podem ser desinfetados será aplicada.
CORR–	**Corrompido**.	O aplicativo poderia acessar o objeto, mas ele não pôde ser verificado porque está corrompido (por exemplo, a estrutura do arquivo está corrompida ou o formato do arquivo é inválido). É possível encontrar informações sobre o processamento do objeto no relatório de funcionamento do aplicativo.
WARN–	**Suspeito**. O objeto suspeito contém o código de um vírus desconhecido. A desinfecção não é possível.	O objeto foi considerado suspeito pelo analisador de código heurístico. No momento da detecção, os bancos de dados do aplicativo não contêm uma descrição do procedimento para neutralizar esse objeto. Você será notificado quando um objeto desse tipo for detectado.

Prefixo	Status do objeto	Informação sobre o processamento do objeto
SUSP–	**Suspeito**. O objeto suspeito contém o código de um vírus conhecido. A desinfecção não é possível.	O aplicativo detectou uma correspondência parcial entre uma seção do código do objeto e uma seção do código de um vírus conhecido. No momento da detecção, os bancos de dados do aplicativo não contêm uma descrição do procedimento para neutralizar esse objeto. Você será notificado quando um objeto desse tipo for detectado.
ERRO–	**Erro de varredura**.	Ocorreu um erro ao verificar o objeto. O aplicativo não pôde acessar o objeto: a integridade do objeto foi violada (por exemplo, um arquivo comprimido de vários volumes não tem fim) ou não é possível conectá-lo (se o objeto verificado estiver localizado em uma unidade de rede). Você pode encontrar informações sobre o processamento do objeto no relatório de funcionamento do aplicativo.
CURE–	**Infectado**. O objeto infectado contém o código de um vírus conhecido. É possível desinfetá-lo.	O objeto contém um vírus que pode ser desinfetado. O aplicativo desinfetará o objeto; o texto do corpo do “vírus” será substituído pela palavra CURE. Você será notificado quando um objeto desse tipo for detectado.

Prefixo	Status do objeto	Informação sobre o processamento do objeto
DELE–	**Infectado**. O objeto infectado contém o código de um vírus conhecido. A desinfecção não é possível.	O aplicativo identifica o objeto como um vírus que não pode ser desinfetado. Ocorre um erro ao tentar desinfetar o objeto; a ação executada será aquela especificada para objetos que não podem ser desinfetados. Você será notificado quando um objeto desse tipo for detectado.

TESTANDO A PROTEÇÃO DO TRÁFEGO HTTP

- *Para verificar se os vírus nos fluxos de dados transferidos pelo protocolo HTTP são detectados com êxito:*

  Tente baixar um "vírus" de teste do site oficial da organização EICAR em: http://www.eicar.org/anti_virus_test_file.htm.

Ao tentar baixar o "vírus" de teste, o Kaspersky Internet Security detectará esse objeto, o identificará como um objeto infectado que não pode ser desinfetado e executará a ação especificada nas configurações de tráfego HTTP para objetos com esse status. Por padrão, quando você tentar baixar o "vírus" de teste, a conexão com o site será encerrada e o navegador exibirá uma mensagem informando ao usuário que esse objeto está infectado com o vírus EICAR-Test-File.

TESTANDO A PROTEÇÃO DO TRÁFEGO SMTP

Para detectar vírus em fluxos de dados transferidos através do protocolo SMTP, é necessário transferir os dados usando um sistema de e-mail que utilize esse protocolo.

> Observação
>
> É recomendável testar como o Kaspersky Internet Security trata as mensagens de e-mail enviadas e recebidas, incluindo o corpo das mensagens e os anexos. Para testar a detecção de vírus no corpo das mensagens, copie o texto do "vírus" de teste padrão ou do "vírus" modificado no corpo da mensagem.

- *Para testar a detecção de vírus em fluxos de dados SMTP:*

1. Crie uma mensagem no formato de **texto sem formatação** usando um programa de e-mail instalado no computador.

   > Observação
   >
   > A mensagem que contém um vírus de teste não será verificada se for criada no formato RTF ou HTML.

2. Copie o texto do "vírus" padrão ou modificado no início da mensagem ou anexe um arquivo contendo o "vírus" de teste à mensagem.

3. Envie a mensagem ao administrador.

O aplicativo irá detectar o objeto, identificá-lo como infectado e bloquear a mensagem.

VALIDANDO AS CONFIGURAÇÕES DE ARQUIVOS E MEMÓRIA

- *Para verificar se o componente Arquivos e memória está configurado corretamente:*

1. Crie uma pasta em um disco e copie nela o “vírus” de teste da EICAR que você baixou e os “vírus” de teste modificados que criou.

2. Certifique-se de que todos os eventos sejam registrados, de forma que o arquivo do relatório contenha os dados de objetos corrompidos e de objetos não verificados devido a erros.

3. Execute o "vírus" de teste ou alguma de suas versões modificadas.

O componente Arquivos e memória interceptará a chamada do arquivo, o verificará e executará a ação especificada nas configurações para objetos com esse status. Ao selecionar a execução de outras ações com o objeto detectado, você poderá verificar o funcionamento do componente.

As informações sobre os resultados da operação do componente Arquivos e memória podem ser visualizadas no relatório de funcionamento do componente.

VALIDANDO AS CONFIGURAÇÕES DA TAREFA DE VARREDURA DE VÍRUS

- *Para verificar se a tarefa de varredura de vírus foi configurada corretamente:*

1. Crie uma pasta em um disco e copie nela o “vírus” de teste da EICAR que você baixou e os “vírus” de teste modificados que criou.

2. Crie uma nova tarefa de varredura de vírus e selecione a pasta que contém o conjunto de “vírus” de teste como o objeto a ser verificado.

3. Certifique-se de que todos os eventos sejam registrados, de forma que o arquivo do relatório contenha os dados de objetos corrompidos e de objetos não verificados devido a erros.

4. Execute a tarefa de varredura de vírus.

Quando a tarefa de varredura estiver sendo executada, as ações especificadas nas configurações de tarefa serão realizadas conforme objetos suspeitos ou infectados sejam detectados. Você poderá realizar uma verificação completa do funcionamento do componente selecionando várias ações a serem executadas com objetos detectados.

Todas as informações sobre as ações da tarefa podem ser visualizadas no relatório de funcionamento do componente.

VALIDANDO AS CONFIGURAÇÕES DO ANTI-SPAM

Você pode usar uma mensagem como teste identificada como SPAM para testar a proteção do Anti-Spam.

O corpo da mensagem de teste deve conter a seguinte linha:

```
Spam is bad do not send it
```

Quando essa mensagem for recebida no computador, o aplicativo a verificará, atribuirá o status “spam” a ela e executará a ação especificada para objetos desse tipo.

DECLARAÇÃO SOBRE COLETA DE DADOS DO KASPERSKY SECURITY NETWORK

INTRODUÇÃO

LEIA ESTE DOCUMENTO COM ATENÇÃO. ELE CONTÉM INFORMAÇÕES IMPORTANTES QUE VOCÊ DEVE SABER ANTES DE CONTINUAR A USAR NOSSOS SERVIÇOS OU SOFTWARES. A CONTINUIDADE DO USO DE SOFTWARES E SERVIÇOS DA KASPERSKY LAB SERÁ CONSIDERADA COMO A SUA ACEITAÇÃO DESTA DECLARAÇÃO SOBRE Coleta de Dados DA KASPERSKY LAB. Nos reservamos o direito de modificar esta Declaração sobre Coleta de Dados a qualquer momento, ao publicar as alterações nesta página. Verifique a data de revisão a seguir para determinar se a política foi modificada desde que a última vez que a analisou. A continuidade do uso de qualquer parte dos serviços da Kaspersky Lab depois da publicação da Declaração sobre Coleta de Dados atualizada constituirá sua aceitação das modificações.

A Kaspersky Lab e seus afiliados (coletivamente chamados, "***Kaspersky Lab***") criaram esta Declaração sobre Coleta de Dados para informar e divulgar suas práticas de coleta e distribuição de dados do Kaspersky Anti-Virus e do Kaspersky Internet Security.

Palavra da Kaspersky Lab

A Kaspersky Lab tem o compromisso de fornecer excelentes serviços a todos os nossos clientes, respeitando especialmente suas preocupações com relação à Coleta de Dados. Entendemos que você pode ter dúvidas sobre como o Kaspersky Security Network coleta e usa informações e dados, e preparamos esta declaração para informá-lo sobre os princípios da Coleta de Dados que norteiam o Kaspersky Security Network (a "***Declaração sobre Coleta de Dados***" ou "***Declaração***").

A Declaração sobre Coleta de Dados contém vários detalhes gerais e técnicos sobre as medidas tomadas para respeitar suas preocupações quanto à Coleta de Dados. Esta Declaração sobre Coleta de Dados está organizada de acordo com os principais processos e áreas, para que você possa analisar rapidamente

as informações de seu interesse. Atender às suas necessidades e expectativas é a base de tudo o que fazemos – inclusive proteger sua Coleta de Dados.

Os dados e as informações são coletados pela Kaspersky Lab. Se, depois de analisar esta Declaração sobre Coleta de Dados, você tiver dúvidas ou preocupações com relação ao assunto, envie um e-mail para support@kaspersky.com.

O que é o Kaspersky Security Network?

O serviço Kaspersky Security Network permite aos usuários dos produtos de segurança da Kaspersky Lab em todo o mundo ajudar a facilitar a identificação e reduzir o tempo que se leva para fornecer proteção contra novos riscos de segurança ("em campo") que visam seu computador. Para identificar novas ameaças e suas fontes e para ajudar a melhorar a segurança do usuário e a funcionalidade do produto, o Kaspersky Security Network coleta dados selecionados de segurança e de aplicativos sobre possíveis riscos de segurança que visam seu computador, e envia esses dados à Kaspersky Lab para análise. **Essas informações não contêm informações de identificação pessoal do usuário e são utilizadas pela Kaspersky Lab somente com a finalidade de melhorar seus produtos de segurança e aprimorar ainda mais as soluções contra ameaças maliciosas e vírus. No caso de transmissão acidental de dados pessoais do usuário, a Kaspersky Lab os manterá e protegerá de acordo com esta Declaração sobre Coleta de Dados**.

Ao participar do Kaspersky Security Network, você e outros usuários dos produtos de segurança da Kaspersky Lab em todo o mundo contribuem significativamente para um ambiente de Internet mais seguro.

Questões legais

O Kaspersky Security Network pode estar sujeito às leis de várias jurisdições, pois seus serviços podem ser usados em jurisdições diferentes, incluindo os Estados Unidos da América. A Kaspersky Lab poderá divulgar informações de identificação pessoal sem a sua permissão quando exigido por lei, ou na crença de boa-fé que isso seja necessário na investigação ou proteção contra atividades perigosas dos visitantes, convidados, associados ou a propriedade da Kaspersky Lab ou de outros. Como mencionado acima, as leis relacionadas aos dados e às informações coletados pelo Kaspersky Security Network podem variar de acordo com o país. Por exemplo, algumas informações de identificação pessoal coletadas na União Européia e seus estados membros estão sujeitas às Diretrizes da UE relacionadas aos dados pessoais, privacidade e comunicações eletrônicas, incluindo mas não se limitando à Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa aos dados pessoais e a proteção da privacidade no setor de comunicações eletrônicas, a Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 sobre a proteção de indivíduos com relação ao processamento de dados

pessoais e ao livre movimento de tais dados, a legislação subseqüente adotada nos estados membros da União Européia, a Decisão da Comissão Européia 497/2001/CE sobre cláusulas contratuais padrão (dados pessoais transferidos aos países do terceiro mundo) e a legislação subseqüente adotada nos estados membros da Comunidade Européia.

O Kaspersky Security Network informará oportunamente os usuários envolvidos quando começar a coletar as informações mencionadas acima, sobre qualquer compartilhamento dessas informações, especialmente para o desenvolvimento de negócios e permitirá a esses usuários da Internet **consentir** (opt-in) (nos estados membros da CE e outros países que exijam o procedimento opt-in) ou recusar (opt-out) on-line (para todos os outros países) o uso comercial destes dados e/ou a transmissão destes dados a terceiros.

Pode ser exigido por imposição da lei ou das autoridades judiciárias que a Kaspersky Lab forneça informações de identificação pessoal às autoridades governamentais pertinentes. Caso seja solicitado por imposição da lei ou das autoridades judiciárias, forneceremos essas informações mediante recebimento de documentação apropriada. A Kaspersky Lab pode também fornecer informações por imposição da lei para proteger suas propriedades e a integridade e segurança dos indivíduos conforme permitido por lei.

As declarações às autoridades dos estados membros sobre Proteção de Dados Pessoais serão feitas de acordo com a legislação em vigor nos estados membros da UE. As informações sobre tais declarações poderão ser acessadas através dos serviços do Kaspersky Security Network.

INFORMAÇÕES COLETADAS

Dados que coletamos

O serviço do Kaspersky Security Network coletará e enviará à Kaspersky Lab dados básicos e ampliados sobre possíveis riscos de segurança direcionados ao seu computador. Os dados coletados incluem:

Dados básicos

- informações sobre o hardware e software de seu computador, incluindo o sistema operacional e service packs instalados, objetos de kernel, drivers, serviços, extensões do Internet Explorer, extensões de impressão, extensões do Windows Explorer, arquivos de programas baixados, elementos de configuração ativa, applets do painel de controle, registros de hospedagem e do sistema, endereços IP, tipos de navegadores, programas de e-mail e o número da versão do produto da Kaspersky Lab que, em geral, não fornece uma identificação pessoal;

- uma identificação exclusiva que não contém nenhuma informação pessoal é gerada pelo produto da Kaspersky Lab para identificar computadores individuais sem identificar o usuário;

- informações sobre o status da proteção antivírus de seu computador e dados sobre os arquivos ou atividades suspeitas de ser malware (por exemplo, nome de vírus, data/hora de detecção, nomes/caminhos e tamanho dos arquivos infectados, IP e porta de ataque de rede, nome do aplicativo suspeito de ser malware). Os dados coletados mencionados acima não contêm informações de identificação pessoal.

Dados ampliados

- Informações sobre aplicativos assinados digitalmente baixados pelo usuário (URL, tamanho do arquivo, nome do signatário);

- Informações sobre aplicativos executáveis (tamanho, atributos, data de criação, informações sobre cabeçalhos PE, região, nome, localidade e utilitário de compactação usado).

Protegendo a transmissão e o armazenamento de dados

A Kaspersky Lab tem o compromisso de proteger a segurança das informações que coleta. As informações coletadas são armazenadas em servidores com acesso limitado e controlado. A Kaspersky Lab possui redes de dados seguros protegidas por sistemas de proteção por senha e firewall padrão do setor. Utilizamos uma diversas tecnologias e procedimentos de segurança para proteger as informações coletadas contra ameaças como acesso, utilização ou divulgação não-autorizada. Nossas políticas de segurança são revistas periodicamente e melhoradas conforme necessário, e somente pessoas autorizadas têm acesso aos dados coletados. A Kaspersky Lab toma medidas para assegurar que suas informações sejam manipuladas de forma segura e de acordo com esta Declaração. Infelizmente, nenhuma transmissão de dados é absolutamente segura. Por isso, apesar de nos empenharmos em proteger seus dados, não podemos garantir a segurança de dados que você nos transmite ou de nossos produtos ou serviços, incluindo, sem limitação, o Kaspersky Security Network; assim, ao utilizar esses serviços, você assume essa responsabilidade.

Os dados coletados devem ser transferidos para os servidores da Kaspersky Lab e a Kaspersky Lab toma as precauções necessárias para assegurar que as informações coletadas, se transferidas, recebam um nível de proteção apropriado. Tratamos os dados que coletamos como informações confidenciais; conseqüentemente, eles estão sujeitos aos nossos procedimentos de segurança e políticas corporativas em relação à proteção e ao uso de informações confidenciais. Depois que os dados coletados chegam à Kaspersky Lab, eles são armazenados em um servidor com recursos de segurança eletrônicos e físicos comuns no setor, incluindo a utilização de procedimentos de login/senha e firewalls eletrônicos projetados para bloquear o acesso não-autorizado de fora

da Kaspersky Lab. Os dados coletados pelo Kaspersky Security Network cobertos por esta Declaração são processados e armazenados nos Estados Unidos e possivelmente em outras jurisdições, como também em países nos quais a Kaspersky Lab realiza negócios. Todos os funcionários da Kaspersky Lab estão cientes de nossas políticas de segurança. Seus dados são acessíveis somente aos funcionários que precisam deles para executar seus trabalhos. Nenhum dado armazenado será associado com informações de identificação pessoal. A Kaspersky Lab não faz a correspondência entre os dados armazenados pelo Kaspersky Security Network e outros dados, listas de contatos ou informações de assinaturas coletados pela Kaspersky Lab para fins promocionais ou outros.

USO DOS DADOS COLETADOS

Como suas informações pessoais são usadas

A Kaspersky Lab coleta os dados para analisar e identificar a fonte de possíveis riscos de segurança e para melhorar a capacidade dos produtos da Kaspersky Lab de detectar comportamento malicioso, sites fraudulentos, crimeware e outros tipos de ameaças de segurança da Internet, de forma a fornecer o melhor nível de proteção possível aos clientes da Kaspersky Lab.

Divulgação de informações a terceiros

A Kaspersky Lab pode divulgar qualquer informação coletada se lhe for solicitado por um oficial da lei, conforme exigido ou permitido por lei, ou em resposta a uma intimação ou outros processos legais, ou se acreditarmos de boa-fé que somos obrigados a tal para cumprir com as leis, regulamentos de intimação outros ou processos legais aplicáveis ou uma solicitação governamental compulsória. A Kaspersky Lab também pode divulgar informações de identificação pessoal, quando tivermos motivos para acreditar que a divulgação dessas informações seja necessária para identificar, entrar em contato ou entrar com uma ação judicial contra quem possa estar violando esta Declaração, os termos de nossos contratos com a Empresa, ou para proteger a segurança de nossos usuários e do público, ou mediante acordos de confidencialidade e de licença com terceiros que nos assistem no desenvolvimento, operação e manutenção do Kaspersky Security Network. Com o intuito de promover a conscientização, a detecção e a prevenção de riscos à segurança da Internet, a Kaspersky Lab pode compartilhar determinadas informações com organizações de pesquisa e outros fornecedores de software de segurança. A Kaspersky Lab também pode fazer uso de estatísticas derivadas das informações coletadas para acompanhar e publicar relatórios sobre tendências dos riscos de segurança.

As opções disponíveis para você

A participação no Kaspersky Security Network é opcional. Você pode ativar e desativar o serviço Kaspersky Security Network a qualquer momento, visitando as configurações de Feedback na página de configurações do produto da Kaspersky Lab. Porém, se você optar por reter as informações ou os dados solicitados, talvez não possamos fornecer-lhe alguns dos serviços que dependem da coleta desses dados.

Ao final do período de serviço de seu produto da Kaspersky Lab, algumas das funções do software da Kaspersky Lab podem continuar funcionando, mas as informações não serão mais enviadas automaticamente para a Kaspersky Lab.

Também nos reservamos o direito de enviar mensagens de alerta esporádicas aos usuários para informá-los sobre mudanças específicas que possam influenciar no uso dos serviços que eles assinaram anteriormente. Também nos reservamos o direito de entrar em contato com você, caso sejamos forçados a tal como parte de um procedimento legal ou se houver a violação de alguma licença, garantia e contratos de compra aplicáveis.

A Kaspersky Lab se reserva esses direitos porque, em casos limitados, devemos ter o direito de entrar em contato com você, em questões legais ou relacionadas a questões que podem ser importantes para você. Esses direitos não nos permitem entrar em contato com você para comercializar serviços novos ou existentes, caso você tenha solicitado que não o façamos, e a emissão desses tipos de comunicação é rara.

COLETA DE DADOS – CONSULTAS E RECLAMAÇÕES RELACIONADAS

A Kaspersky Lab recebe e trata das preocupações de seus usuários voltadas à Coleta de Dados com o maior respeito e atenção. Se você achar que houve um caso de não conformidade com esta Declaração no que diz respeito às suas informações ou dados, ou se tiver outras consultas ou preocupações relacionadas, escreva ou entre em contato com a Kaspersky Lab pelo e-mail: support@kaspersky.com.

Em sua mensagem, descreva a natureza de sua consulta da forma mais detalhada possível. Investigaremos sua consulta ou reclamação imediatamente.

O fornecimento de informações é voluntário. A opção de coleta de dados pode ser desabilitada pelo usuário a qualquer momento na seção "**Feedback**" da página "**Configurações**" do seu produto Kaspersky.

KASPERSKY LAB

Fundada em 1997, a Kaspersky Lab é conhecida como líder no segmento de tecnologias de segurança da informação. A empresa produz uma grande variedade de software de segurança de dados de alto desempenho, incluindo sistemas antivírus, anti-spam e anti-hacking.

A Kaspersky Lab é uma empresa internacional. Sediada na Federação Russa, a empresa possui escritórios no Reino Unido, França, Alemanha, Japão, Holanda, China, Polônia, Romênia e EUA (Califórnia). Um novo escritório da empresa foi aberto recentemente na França, o Centro Europeu de Pesquisa Antivírus. A rede de parceiros da Kaspersky Lab inclui mais de 500 empresas no mundo inteiro.

Atualmente, a Kaspersky Lab emprega mais de 450 especialistas altamente qualificados, incluindo 10 detentores de mestrado e 16 detentores de PhD. Vários especialistas em antivírus da Kaspersky Lab fazem parte da CARO (Computer Anti-Virus Researchers Organization).

Os ativos mais valiosos de nossa empresa são o conhecimento exclusivo e a especialização acumulada por seus especialistas durante os 14 anos em que combatemos continuamente os vírus de computador. Uma análise completa das atividades de vírus de computador permite aos especialistas da empresa prever as tendências de desenvolvimento de malware e fornecer aos nossos usuários uma proteção oportuna contra os novos tipos de ataques. A resistência a ataques futuros é a diretiva básica implementada em todos os produtos da Kaspersky Lab. Os produtos da empresa estão sempre um passo à frente de outros fornecedores no fornecimento de proteção antivírus aos clientes.

Os anos de muito trabalho tornaram a empresa um dos principais desenvolvedores de software antivírus. A Kaspersky Lab foi uma das primeiras empresas do segmento a desenvolver vários padrões de software antivírus modernos. O principal produto da empresa, o Kaspersky Anti-Virus, fornece proteção integral para todos os níveis de uma rede: estações de trabalho, servidores de arquivos, sistemas de e-mail, firewalls, gateways da Internet e computadores portáteis. Suas ferramentas de gerenciamento convenientes e fáceis de usar maximizam o nível de automação da proteção antivírus de computadores e redes corporativas. Vários fabricantes conhecidos usam o kernel do Kaspersky Anti-Virus, incluindo Nokia ICG (EUA), F-Secure (Finlândia), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab recebem vários serviços adicionais que asseguram o funcionamento estável dos produtos da empresa e a conformidade total com seus requisitos empresariais específicos. Nós projetamos,

implementamos e damos suporte a sistemas corporativos de antivírus. O banco de dados de antivírus da Kaspersky Lab é atualizado de hora em hora. A empresa fornece aos seus clientes serviço de suporte técnico 24 horas em vários idiomas.

Caso tenha alguma dúvida, você pode entrar em contato com nossos distribuidores ou diretamente com a Kaspersky Lab. Consultas detalhadas são fornecidas pelo telefone ou e-mail. Você receberá respostas completas e abrangentes para qualquer pergunta.

Endereço:	Rússia, 123060, Moscou, 1-st Volokolamsky Proezd, 10, Building 1
Fone, Fax:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
Suporte de emergência 24x7:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Suporte para usuários de produtos empresariais:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (das 10 às 19 horas) http://support.kaspersky.com/helpdesk.html
Suporte para usuários corporativos:	as informações de contato serão fornecidas quando você comprar um software corporativo, dependendo de seu pacote de suporte.
Fórum da Kaspersky Lab na Web:	http://forum.kaspersky.com
Laboratório de Antivírus:	newvirus@kaspersky.com (somente para o envio de novos vírus em arquivos comprimidos)
Grupo de desenvolvimento de documentação do usuário:	docfeedback@kaspersky.com (somente para o envio de feedback sobre a documentação e o sistema de Ajuda)
Departamento de vendas:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com

Informações gerais:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com
Internet:	http://www.kaspersky.com.br http://www.viruslist.com

CRYPTOEX LLC

O Kaspersky Anti-Virus utiliza a biblioteca de software de segurança de dados da Crypto Ex LLC, Crypto C, na criação e verificação de assinaturas digitais.

A Crypto Ex detém uma licença da Agência Federal para Comunicações e Informações do Governo (uma subsidiária do FSB – Federal Security Service) para desenvolvimento, fabricação e distribuição de software de criptografia para proteger dados que não constituem segredo de estado.

A biblioteca Crypto C foi projetada para proteger informações confidenciais de classe KS1, tendo recebido o certificado de conformidade do FSB Nº SF/114-0901 em 1º de julho de 2006.

A biblioteca criptografa e descriptografa fluxos de dados e/ou pacotes de dados de tamanho fixo utilizando as seguintes tecnologias:

- um algoritmo de criptografia (GOST 28147-89);
- algoritmos para a geração e verificação de assinaturas digitais baseadas em algoritmos (GOST R 34.10-94 e GOST 34.10-2001);
- funções de hash (GOST 34.11-94);
- geração de informações-chave utilizando um transmissor de programas de números pseudo-aleatórios;
- um sistema de geração de vetor de simulação e informações-chave (GOST 28147-89).

Os módulos da biblioteca foram implementados em ANSI padrão C e podem ser integrados em aplicativos como código carregado estaticamente ou dinamicamente. Ela pode ser executada em diversas plataformas, incluindo x86, x86-64, Ultra SPARC II e outras plataformas compatíveis.

Os módulos de biblioteca podem ser migrados para os seguintes ambientes operacionais: Microsoft Windows NT/XP/98/2000/2003, Unix (Linux, FreeBSD, SCO Open Unix 8.0, SUN Solaris, SUN Solaris para Ultra SPARC II).

Para obter mais informações, visite o site corporativo da CryptoEx LLC em http://www.cryptoex.ru ou entre em contato com a empresa através do e-mail info@cryptoex.ru

MOZILLA FOUNDATION

A biblioteca **Gecko SDK ver. 1.8** foi usada no desenvolvimento dos componentes deste aplicativo.

Este software é usado de acordo com os termos e condições da licença MPL 1.1 Licença pública da Mozilla Foundation http://www.mozilla.org/MPL.

Para obter mais detalhes sobre a biblioteca Gecko SDK, consulte: http://developer.mozilla.org/en/docs/Gecko_SDK.

Site da Mozilla Foundation: http://www.mozilla.org.

CONTRATO DE LICENÇA

Contrato de Licença do Usuário Final Padrão

AVISO A TODOS OS USUÁRIOS: LEIA CUIDADOSAMENTE O SEGUINTE CONTRATO LEGAL ("CONTRATO") RELATIVO À LICENÇA DO KASPERSKY INTERNET SECURITY ("SOFTWARE"), PRODUZIDO PELA KASPERSKY LAB ("KASPERSKY LAB").

SE VOCÊ ADQUIRIU ESTE SOFTWARE PELA INTERNET, CLICANDO NO BOTÃO ACEITAR, VOCÊ (SEJA UM INDIVÍDUO OU UMA ENTIDADE ÚNICA) CONCORDA EM LIMITAR-SE E TORNAR-SE PARTE NESTE CONTRATO. SE NÃO CONCORDAR COM TODOS OS TERMOS DO PRESENTE CONTRATO, CLIQUE NO BOTÃO QUE INDICA QUE NÃO ACEITA OS TERMOS DO CONTRATO E NÃO INSTALE O SOFTWARE.

SE VOCÊ ADQUIRIU ESTE SOFTWARE EM UMA MÍDIA FÍSICA, AO QUEBRAR O LACRE DO CD, VOCÊ (SEJA UM INDIVÍDUO OU UMA ENTIDADE ÚNICA) CONCORDA EM LIMITAR-SE E TORNAR-SE PARTE NESTE CONTRATO. SE NÃO CONCORDA COM TODOS OS TERMOS DESTE CONTRATO, NÃO QUEBRE O LACRE DO CD, NÃO FAÇA DOWNLOAD, NÃO INSTALE NEM USE ESTE SOFTWARE.

DE ACORDO COM A LEGISLAÇÃO RELATIVA AO SOFTWARE DA KASPERSKY DESTINADO A CONSUMIDORES INDIVIDUAIS E COMPRADO ON-LINE NO SITE DA KASPERSKY LAB OU DE SEUS PARCEIROS, O CLIENTE DEVERÁ TER UM PERÍODO DE CATORZE (14) DIAS ÚTEIS A PARTIR DA ENTREGA DO PRODUTO PARA DEVOLVÊ-LO AO REVENDEDOR PARA TROCA OU REEMBOLSO, DESDE QUE O SOFTWARE ESTEJA SELADO.

COM RELAÇÃO AO SOFTWARE DA KASPERSKY DESTINADO A CONSUMIDORES INDIVIDUAIS NÃO ADQUIRIDO ON-LINE, PELA INTERNET, ESSE SOFTWARE NÃO PODERÁ SER DEVOLVIDO OU TROCADO, EXCETO POR PROVISÕES EM CONTRÁRIO ESTABELECIDAS PELO PARCEIRO QUE COMERCIALIZA O PRODUTO. NESTE CASO, A KASPERSKY LAB NÃO ESTARÁ SUJEITA ÀS CLÁUSULAS DO PARCEIRO.

O DIREITO DE DEVOLUÇÃO E REEMBOLSO SE ESTENDE APENAS AO COMPRADOR ORIGINAL.

Todas as referências na presente a "Software" devem ser consideradas como incluindo o código de ativação do software, que será fornecido pela Kaspersky Lab como parte do Kaspersky Internet Security.

1. *Concessão de Licença*. Sujeito ao pagamento das taxas de licença aplicáveis e sujeito aos termos e condições deste Contrato, a Kaspersky Lab concede a você, por meio da presente, o direito não exclusivo e intransferível de usar o Software e a documentação que o acompanha (a “Documentação”) durante a vigência deste Contrato, unicamente para seus próprios fins comerciais internos. Você pode instalar uma cópia do Software em um computador.

1.1 *Uso*. Caso o Software tenha sido adquirido em uma mídia física, você tem o direito de usá-lo para a proteção do número de computadores indicado na caixa. Caso o Software tenha sido adquirido pela Internet, você tem o direito de usá-lo para a proteção do número de computadores solicitado no momento da compra.

1.1.1 O Software está “em uso” em um computador quando está carregado na memória temporária (ou seja, a memória RAM) ou instalado na memória permanente (por exemplo, no disco rígido, no CD-ROM ou em outro dispositivo de armazenamento) desse computador. Esta licença o autoriza a fazer quantas cópias de backup do Software forem necessárias para sua utilização dentro dos termos da lei e unicamente para fins de backup, desde que todas essas cópias contenham todos os avisos sobre propriedade do Software. Você deverá manter registros do número e do local de todas as cópias do Software e da Documentação, e deverá adotar todas as precauções necessárias para proteger o Software de uso ou cópia não autorizados.

1.1.2 O Software protege o computador contra vírus e ataques de rede cujas assinaturas estão contidas nos bancos de dados de assinaturas de ameaças e ataques de rede disponíveis nos servidores de atualização da Kaspersky Lab.

1.1.3 Se você vender o computador no qual o Software está instalado, deverá verificar se todas as cópias do Software foram previamente excluídas.

1.1.4 Você não deverá descompilar, aplicar engenharia reversa, desmontar ou reduzir de qualquer outra forma qualquer parte deste Software a um formato legível, nem permitir que qualquer terceiro o faça. As informações de interface necessárias para obter a interoperabilidade do Software com programas de computador criados independentemente serão fornecidas pela Kaspersky Lab quando solicitado, mediante pagamento dos custos plausíveis e das despesas relativas à busca e ao fornecimento dessas informações. No caso de a Kaspersky Lab o notificar de que não pretende disponibilizar essas informações por qualquer motivo, incluindo custos (sem limitações), deverá ser permitido que você tome as medidas necessárias para conseguir a interoperabilidade, desde que seja feita a engenharia reversa ou descompilação do Software apenas até os limites permitidos pela lei.

1.1.5 Você não poderá fazer correções de erros ou de alguma outra forma modificar, adaptar ou converter o Software, nem criar trabalhos derivados do mesmo, nem permitir que terceiros o copiem (a menos que expressamente permitido pelo presente).

1.1.6 Você não poderá alugar, locar ou emprestar o Software a terceiros, nem transferir ou sublicenciar seus direitos de licença a qualquer outra pessoa.

1.1.7 Você não poderá fornecer o código de ativação ou o arquivo da chave de licença a terceiros, nem permitir que terceiros tenham acesso a eles. O código de ativação e a chave de licença constituem-se em dados confidenciais.

1.1.8 A Kaspersky Lab pode solicitar que você instale a versão mais recente do Software (a versão e o pacote de manutenção mais recentes).

1.1.9 Você não deverá usar este Software em ferramentas automáticas, semi-automáticas ou manuais projetadas para criar assinaturas de vírus, rotinas de detecção de vírus, qualquer outro código ou dados para detecção de código ou dados mal-intencionados.

1.1.10 A Kaspersky Lab, com o seu consentimento confirmado explicitamente na Declaração correspondente, tem o direito de coletar informações sobre possíveis ameaças e vulnerabilidades em seu computador. As informações assim coletadas são usada de forma genérica com o único propósito de melhorar os produtos da Kaspersky Lab.

2. *Suporte* [1].

(i) A Kaspersky Lab fornecerá serviços de suporte ("Serviços de Suporte") conforme definido a seguir, por um período especificado no arquivo da chave de licença (período do serviço) e indicado na janela "Serviço", a partir do momento da ativação, desde:

(a) o pagamento dos então atuais encargos de suporte e;

(b) o preenchimento bem-sucedido do Formulário de Assinatura de Serviços de Suporte, conforme fornecido com este Contrato ou conforme disponível no site da Kaspersky Lab, que exigirá que você insira o código de ativação também fornecido a você pela Kaspersky Lab com este Contrato. À sua total discrição, a

[1] Ao usar o software de demonstração, você não tem direito ao Suporte Técnico especificado na Cláusula 2 deste EULA, nem o direito de vender essa cópia a terceiros.

Você tem o direito de usar o software para fins de demonstração, durante o período especificado no arquivo da chave de licença, a partir do momento da ativação (esse período pode ser visualizado na janela Serviço da interface do usuário do software).

Kaspersky Lab decidirá se você satisfez ou não esta condição para a provisão dos Serviços de Suporte.

Os Serviços de Suporte estarão disponíveis após a ativação do Software. O serviço de suporte técnico da Kaspersky Lab também tem o direito de solicitar de você um registro adicional para a concessão de identificador para o processamento de Serviços de Suporte.

Até a ativação do Software e/ou a obtenção do identificador do Usuário Final (ID do Cliente), o serviço de suporte técnico oferece assistência apenas na ativação do Software e no registro do Usuário Final.

(ii) Os Serviços de Suporte serão encerrados a menos que sejam renovados anualmente com o pagamento dos então atuais encargos de suporte anuais e o novo preenchimento bem-sucedido do Formulário de Assinatura de Serviços de Suporte.

(iii) Por “Serviços de Suporte” entendem-se:

(a) Atualizações periódicas do banco de dados de antivírus;

(b) Atualizações do banco de dados de ataques de rede;

(c) Atualizações do banco de dados de anti-spam;

(d) Atualizações gratuitas de software, incluindo as atualizações de versão;

(e) Suporte técnico pela Internet e pela linha direta de suporte fornecida pelo Fornecedor e/ou Revendedor;

(f) Atualizações de detecção e desinfecção de vírus 24 horas por dia.

(iv) Os Serviços de Suporte serão fornecidos somente se e quando você tiver a versão mais recente do Software (incluindo os pacotes de manutenção), disponível no site oficial da Kaspersky Lab (www.kaspersky.com), instalado no seu computador.

3. *Direitos de Propriedade*. O Software é protegido por leis de direitos autorais. A Kaspersky Lab e seus fornecedores possuem e detêm todos os direitos, títulos de interesses no e para o Software, incluindo todos os direitos autorais, patentes, marcas comerciais e outros direitos de propriedade intelectual relacionados. A posse, instalação ou uso do Software por você não lhe transfere

qualquer título à propriedade intelectual do Software, e você não adquirirá quaisquer direitos ao Software, exceto aqueles expressamente definidos no presente Contrato.

4. *Confidencialidade*. Você concorda que o Software e a Documentação, incluindo o projeto e a estrutura específicos de programas individuais, constituem informações proprietárias confidenciais da Kaspersky Lab. Você não deverá divulgar, fornecer ou disponibilizar de qualquer outra maneira essas informações confidenciais, em qualquer forma, para terceiros, sem o consentimento prévio por escrito da Kaspersky Lab. Você deverá implementar medidas de segurança aceitáveis para proteger essas informações confidenciais mas, sem limitação a isso, deverá usar os melhores meios para manter a segurança do código de ativação.

5. *Garantia Limitada*.

(i) A Kaspersky Lab garante que, por seis (6) meses a partir do primeiro download ou da instalação, o Software adquirido em mídia física terá um desempenho significativamente de acordo com a funcionalidade descrita na Documentação, quando operado corretamente e da forma especificada na Documentação.

(ii) Você assume toda a responsabilidade pela seleção deste Software para preencher seus requisitos. A Kaspersky Lab não garante que o Software e/ou a Documentação serão adequados para suas necessidades, nem que sua utilização será ininterrupta ou isenta de erros.

(iii) A Kaspersky Lab não garante que este Software identifique todos os spams e vírus conhecidos, nem que ocasionalmente o Software não possa relatar erroneamente um vírus em um título não infectado por esse vírus.

(iv) A única solução e toda a responsabilidade da Kaspersky Lab por violações da garantia descrita no parágrafo (i) será, como opção da Kaspersky Lab, que ela repare, substitua ou reembolse o Software, se tal fato for relatado à Kaspersky Lab ou seu representante durante o período da garantia. Você deverá fornecer todas as informações necessárias satisfatórias para auxiliar o Fornecedor na resolução do item com defeito.

(v) A garantia mencionada no parágrafo (i) não se aplicará se você (a) fizer ou causar alterações neste Software sem o consentimento da Kaspersky Lab, (b) usar o Software de uma forma para a qual ele não se destina ou (c) usar o Software de forma diferente daquela permitida por este Contrato.

(vi) As garantias e condições declaradas neste Contrato substituem todas as outras condições, garantias ou outros termos relativos ao fornecimento ou suposto fornecimento de, à falha ou atraso no fornecimento do Software ou da Documentação que podem, exceto por este parágrafo (vi), ter valor entre a Kaspersky Lab e você, ou que de outra forma poderiam estar implícitas ou incorporadas neste Contrato ou em qualquer contrato paralelo, seja por estatuto, pela lei comum ou outra, todos excluídos pela presente (incluindo, sem limitações, as condições, garantias ou outros termos implícitos, como os relativos à qualidade satisfatória, adequação às finalidades ou ao uso de habilidades e cuidados satisfatórios).

6. *Limitação de Responsabilidade*.

(i) Nenhuma parte deste Contrato excluirá ou limitará a responsabilidade da Kaspersky Lab por (a) delitos de fraude, (b) morte ou danos pessoais causados por violações de “duty of care” da lei comum ou de qualquer violação por negligência de um termo deste Contrato ou (c) qualquer outra responsabilidade que não possa ser excluída pela lei.

(ii) Sujeita ao parágrafo (i) acima, a Kaspersky Lab não se responsabilizará (seja por contrato, agravo, restituição ou outros) por nenhuma das seguintes perdas e danos (quer essas perdas e danos tenham sido previstos, previsíveis, conhecidos ou de outra forma):

(a) Perda de rendimentos;

(b) Perda de lucros reais ou previstos (incluindo a perda de lucros em contratos);

(c) Perda do uso de dinheiro;

(d) Perda de economias previstas;

(e) Perda de negócios;

(f) Perda de oportunidades;

(g) Perda de boa-fé;

(h) Perda de reputação;

(i) Perda de, danos a ou corrupção de dados ou:

(j) Qualquer perda ou dano indireto ou conseqüente causado de alguma forma (incluindo, para evitar dúvidas, os casos em que

essas perdas e danos sejam dos tipos especificados nos parágrafos (ii), (a) a (ii), (i).

(iii) Sujeita ao parágrafo acima (i), a responsabilidade da Kaspersky Lab (seja por contrato, agravo, restituição ou outros) decorrente de ou em correlação com o fornecimento do Software em nenhuma circunstância excederá o valor igual ao igualmente pago por você pelo Software.

7. Neste Contrato está contido o entendimento integral entre as partes com relação ao assunto do mesmo, tendo prevalência sobre todos e quaisquer entendimentos, compromissos e promessas anteriores entre você e a Kaspersky Lab, sejam eles orais ou por escrito, que tenham sido definidos ou que possam estar implícitos em qualquer elemento escrito ou declarado nas negociações entre nós ou nossos representantes antes deste Contrato e todos os contratos anteriores entre as partes, relacionados aos assuntos mencionados previamente terão sua validade suspensa a partir da Data de Efetivação.